bitdefender ANTIVIRUS PRO 2011

用户使用指南



BitDefender Antivirus Pro 2011
用户使用指南

出版方 2010.08.10

法律须知


bitdefender

目录

安装和移除

1. 系统需求

您只能在下列操作系统上安装 BitDefender Antivirus Pro 2011:

- Windows XP SP3 (32 位) / Windows XP SP2 (64 位)
- Windows Vista SP1 或更高(32/64 位)
- Windows 7 (32/64位)

在安装之前，请确保您的计算机满足最低的硬件和软件的要求。



注意
想了解您计算机上的Windows操作系统和硬件信息，请在我的电脑点击右键，然后从菜单中选择属性。

1.1. 最低系统需求

- 1GB 可用磁盘空间
- CPU: 800MHz
- 内存:
  - 512MB (Windows XP)
  - 1GB(Windows Vista/Windows 7)
- Internet Explorer 6.0
- .NET Framework 2 (包含在安装包中)
- Adobe Flash Player 10.0.45.2

1.2. 推荐的系统配置

- 1GB 可用磁盘空间
- CPU: Intel 酷睿2 (1.66GHz) 或同级处理器
- 内存:
  - 1GB(Windows XP/Windows 7)
  - 1.5GB(Windows Vista)
- Internet Explorer 7
- .NET Framework 2 (包含在安装包中)
- Adobe Flash Player 10.0.45.2

1.3. 软件需求

反钓鱼欺诈仅可用于下列软件:

- IE浏览器6.0或以上
- Mozilla Firefox 3.x
- 雅虎通8.1
- MSN 8

即时通讯加密仅可用于下列软件:

- 雅虎通8.1
- MSN 8

2. 准备安装

在开始安装 BitDefender Antivirus Pro 2011之前，请完成下述准备工作，以确保安装顺利：

- 请确保您准备安装 BitDefender 的电脑符合最低系统需求。如果电脑没有达到最低系统要求，BitDefender 将无法安装，即便安装也无法正常工作，并导致系统关机或不稳定。欲了解详细的系统需求，请参阅 “系统需求” (第 2 页)。
- 使用系统管理员账号登陆电脑。
- 卸载电脑上的其他安全软件。在一台电脑上同时运行两个安全软件可能导致系统不稳定或异常。Windows Defender 默认情况下在安装开始前将会被禁用。

3. 产品安装

您可用 BitDefender 安装光盘进行安装，或者使用从 BitDefender 网站或其他合作伙伴网站下载的安装文件进行安装。您可从下面的 BitDefender 网站下载安装文件： http://www.bitdefender.com/site/Downloads/。

- 要从光盘安装 BitDefender，请将光盘插入光驱，您将会看到一个欢迎窗口，请遵循提示开始安装。



注意

欢迎屏幕提供了一个选项，可将安装包从光盘复制到U盘。如果您需要为一台没有光驱的电脑（如上网本）安装 BitDefender，这个选项将十分有用。将存储设备插入 USB 口，然后点击 拷贝到U盘。然后，将U盘插入没有光驱的电脑中，并双击U盘上的 runsetup.exe。

如果欢迎窗口未显示，请到光盘的根目录，双击 autorun.exe。

- 要用下载到您电脑上的安装文件进行安装，请双击该文件。

安装程序首先会检查您的系统以验证安装。如果安装已被校验，在安装向导出现之前，您会看到提示您选择语言的窗口。

此向导将帮助您在电脑上安装 BitDefender，同时允许您配置主要设置选项及用户界面。

3.1. 步骤 1 – 介绍

请阅读用户许可协议并选择 我同意 BitDefender 用户许可协议。点击 下一步 继续。

如果您不同意这些条款，请点击 取消 。 将会退出安装进程。

3.2. 步骤 2 – 准备安装

BitDefender 扫描您的电脑，检查是否安装有其他安全软件。

快速扫描

一对您电脑的关键区域进行了快速扫描，以确保电脑中没有活动病毒。

扫描只需几分钟，您可随时点击按钮取消。



重要

强烈建议您允许扫描完成。
活动病毒可能破坏安装甚至导致失败。

扫描结束后会显示结果。如果发现任何安全威胁，请按照提示在继续安装前删除病毒。

点击 下一步 继续。

删除现有的安全软件

如果您的电脑上安装了其他安全软件，BitDefender Antivirus Pro 2011 会警告您。点击对应按钮开始卸载过程，遵循提示卸载产品。



警告
安装BitDefender前，强烈建议您卸载其他杀毒软件。在一台电脑上同时运行两个或两个以上杀毒软件可能使系统瘫痪。

如果 Windows Defender 已启用，建议让 BitDefender 关闭它。

点击 下一步 继续。

3.3. 步骤 3 – 注册

BitDefender注册流程包含用授权密钥注册产品以及创建 BitDefender 账户激活在线功能。

注册产品

根据您的情况继续:

- 我购买了光盘版或在线购买 BitDefender Antivirus Pro 2011

  在此情况下，您需要注册产品:

  1. 在编辑框中输入授权密钥。

     注意
     您可以找到您的授权密钥:
     - 在光盘标签上。
     - 在产品注册卡上。
     - 在网上购买的电子邮件中。

     如果您没有Bitdefender授权密钥，请点击产品中所提供的链接前往Bitdefender网站购买。

  2. 点击 立即注册。
  3. 点击 下一步。

- 我下载 BitDefender Antivirus Pro 2011 试用

  在此情况下，您可使用所有产品功能 30 天。要开始试用，请选择 我要试用 BitDefender Antivirus Pro 2011 30天 并点击 下一步。

激活在线功能

您必须创建一个BitDefender账户，以获得BitDefender更新。该 Bitdefender 账户还可让您获得免费的技术支持、特别优惠和促销产品。如果您丢失 BitDefender 授权密钥，您可在 http://myaccount.bitdefender.com 登录您的账户找回它。

如果您此时并不想创建 BitDefender 账户，请选择 以后创建 并点击 下一步。



注意
如果您安装 BitDefender Antivirus Pro 2011 进行试用，您现在需要创建一个 BitDefender 账户。
如果您购买了此产品，您必须在安装后 30 天内创建一个账户。

否则，根据您当前的情况继续进行：

● 我没有 BitDefender 账户

要成功创建 BitDefender 账户，请遵循下述步骤：

1. 选择 创建新账户。
2. 在对应的输入框中输入所需信息。您在这里提供的信息都将保密。
   - 用户名 – 输入您的电子邮件地址。
   - 密码 – 输入您Bitdefender账户的密码。密码必须在6到16个字符之间。
   - 重输密码 – 再次输入之前指定的密码。

   如果您选择在输入密码时不用密文，则下次就不需重新输入。



注意
账户激活之后，您就可访问 http://myaccount.bitdefender.com 并使用您输入的电子邮件地址和密码登录您的账户。

3. Bitdefender可能会通过您账户的电子邮件地址告知您的特别优惠及促销活动。点击 查看联系人选项 并在出现的窗口中选择一个可用的选项。
   - 给我发送所有消息
   - 给我发送重要信息
   - 不要给我发送任何消息
4. 点击 提交。
5. 点击 下一步 继续。



注意
在使用您的账户之前，您需要激活它。
检查您的电子邮件，并按照 BitDefender 注册服务发给您的邮件中的指示执行操作。

- 我已经有一个BitDefender账户

  Bitdefender会自动检测你这台计算机以前是否注册过Bitdefender账户。在此情况下，请输入您账户的密码并点击 提交。点击 下一步 继续。

  如果您已有有效账号，但是 BitDefender 没有检测到，请参照下述步骤将产品注册到该账号：

  1. 选择 登录(已有账户)。
  2. 输入您账号的电子邮件和密码。

  注意
  如果您忘记了密码，请点击忘记密码?然后按照说明进行。

  3. Bitdefender可能会通过您账户的电子邮件地址告知您的特别优惠及促销活动。点击 查看联系人选项 并在出现的窗口中选择一个可用的选项。
     - 给我发送所有消息
     - 给我发送重要信息
     - 不要给我发送任何消息
  4. 点击 提交。
  5. 点击 下一步 继续。

3.4. 步骤 4 - 选择视图

您可在此选择安装类型及用户界面视图。

选择安装类型

下列安装选项可用：

- 快速安装 - 如想快速安装，而不用详细配置 BitDefender 设置选项，请选择此选项。
- 自定义安装 - 如想自定义安装及 BitDefender 设置，请选择此项。

要查看安装的视频教程，请点击 获取帮助



注意
要用默认选项安装 BitDefender 并直接进入安装向导的最后一步，请选择 跳过安装。

点击 下一步 继续。

选择安装位置



注意

此步骤仅在您选择 自定义安装 时出现。

默认情况下，BitDefender Antivirus Pro 2011 将会被安装在 C:\Program Files\BitDefender\。如果您想更改安装目录，请点击浏览并选择您要安装BitDefender的文件夹。

您可以和其他 BitDefender 用户共享产品文件及病毒库。这样 BitDefender 更新会进行地更快。如果您不想启用此功能，请选择相应的复选框。



注意

如果此功能启用，任何个人信息都不会被共享。

点击 下一步 继续。

选择用户界面

选择最适合您的用户界面视图模式。BitDefender Antivirus Pro 2011 提供三种用户界面，每一种都针对特定用户类型进行了设计。

基本视图

适合计算机水平不高，希望 BitDefender 自动保护电脑安全而减少打扰。界面简单易用，很少需要用户干预。

您所需要做的只是在 BitDefender 发出提示时修复存在的问题即可，BitDefender 会采用直观的向导来引导您一步步解决问题。此外，您还可执行常用任务，如升级或病毒扫描。

中级视图

您可配置 BitDefender 的主要设置选项，单独修复问题，管理安装在家庭电脑上的 BitDefender 产品，选择监测哪些问题。

专家视图

适用于电脑技术高手，此模式下您可全面配置 BitDefender 的各个功能。您可使用 BitDefender 提供的所有功能保护您的电脑和数据。

选择并点击 下一步 继续。

3.5. 步骤 5 – 配置

您可在此自定义您的产品。

配置选项



注意
只有当您将 BitDefender 界面设置为 专家视图 时才会出现此步骤。

您可在此启用/禁用 BitDefender 两大类功能。要修改设置状态，请点击相应的开关。

● 安全设定

您可在此启用/禁用有关电脑和数据安全的多个产品设置选项。

设置	描述
反病毒	实时防护可确保所有被您或运行于此系统的应用程序所访问的文件已被扫描。
自动更新	自动升级可确保最新的 BitDefender 产品及病毒库文件被定时自动下载并安装。
漏洞检测	自动漏洞检测确保您计算机上的关键软件是最新版本。
反钓鱼	反钓鱼功能实时检测欺诈性质的网页并向您发出警示。
身份控制	个人信息控制帮助您防止个人信息未经您同意被发送到互联网。该功能拦截所有的即时通讯、电子邮件信息及网页内容，阻止您所指定的个人信息被发送到未经授权的接收人（或网址）。
聊天加密	即时通讯加密在您的聊天对象也安装了兼容的 BitDefender 产品及通讯软件时，可以保护你们之间通过雅虎通或MSN进行的通话。

● 常规设定

您可在此启用或禁用影响产品行为及用户体验的设置选项。

设置	描述
游戏模式	游戏模式将临时修改防护设定以降低其在游戏时对您系统性能的影响。
笔记本模式检测	笔记本模式将临时修改防护设定以降低其对您笔记本电池电量的影响。
设定密码	配置密码确保BitDefender的设置选项只能由知道密码的人修改。

设置	描述
	当您启用此选项后，您将被提示配置设置选项密码。在输入框中输入所需的密码并点击 确定 以设置密码。
Bitdefender资讯	启用此选项，您将收到来自BitDefender的重要的公司新闻、产品更新或新的安全威胁信息。
产品通知警报	启用此选项，您将收到信息警报。
扫描活动状态栏	扫描活动条是一个小小的透明的窗口，显示BitDefender 扫描活动的进程。更多信息 请参阅 “扫描活动状态栏” （第 18 页）。
发送病毒报告	启用此选项，病毒扫描报告将会被发送给Bitdefender实验室进行分析。请注意，这些报告将不包含机密资料，如您的姓名或IP地址，也不会被用作商业用途。
爆发检测	启用此选项，有关潜在病毒爆发的报告会被发送到Bitdefender实验室进行分析。请注意，这些报告将不包含机密资料，如您的姓名或IP地址，也不会被用作商业用途。

点击 下一步 继续。

配置我的工具



注意
只有当您将 BitDefender 界面设置为 基本视图 或 中级视图 时才会出现此步骤。

使用 我的工具，您可个性化图表板，添加您认为最重要的快捷方式。这样您将能方便地访问它们。

您可在此窗口添加如下工具的快捷方式:

- 游戏模式 – 设置 BitDefender 在您玩游戏时不打扰您。
- 笔记本模式 – 暂时修改防护设置以对电池电量影响最小。
- 家庭网络管理 – 从一台电脑上管理所有安装在您家庭网络电脑上的 BitDefender 产品。
- 全面系统扫描 – 对整个电脑进行扫描。

选择您想添加的工具并点击 下一步 继续。

家庭网络管理



注意
此步骤仅当您将“家庭网络管理”添加到“我的工具”时出现。

您可从下面三个选项中选择一个：

- 将此电脑设置为“服务器”

  如想通过家庭网络中的其他电脑管理 BitDefender 产品，请选择此选项。

  要加入网络需输入密码。在文本框中输入密码并点击 提交。

- 将此电脑设置为“客户端”

  如果 BitDefender 将会被运行着 BitDefender 的家庭网络中的其他电脑管理，请选择此选项。

  要加入网络需输入密码。在文本框中输入密码并点击 提交。

- 暂时跳过安装

  选择此选项稍后从 BitDefender 窗口配置此功能。

点击 下一步 继续。

3.6. 步骤 6 – 支持选项

您可在此自定义帮助及支持选项：

- 启用 / 禁用 智能提示。智能提示是显示在 BitDefender 图表板上的个性化消息，用来帮您提升电脑性能。
- 如需联系 BitDefender 客户服务人员，请确认您将使用的电子邮件地址。如果您不想通过电子邮件与客服人员联系，请选择相应的复选框。

3.7. 步骤 7 – 确认

您可在此复查所选配置。

默认情况下，两个任务会被设定计划：

- 在安装完成后会立即开始进行一次全面系统扫描。

  建议您执行此全面扫描，以发现您电脑上的任何病毒威胁。

- 系统扫描已被计划运行于每周日凌晨 2 点。

  强烈建议您每周至少扫描一次系统。如果默认计划时间不合适，请选择其他日期和时间。如果在计划任务预定运行时间计算机关机，则该任务将在您下次打开计算机时运行。

点击完成。

3.8. 步骤 8 - 完成

安装即将结束，最终设置选项已被应用，并执行了更新。

此向导将在安装完成时自动关闭。如果此选项在上一步被选中，将会运行全面系统扫描。



注意

可能需要重启电脑。

4. 从老版 BitDefender 升级

如果您正在使用 BitDefender Antivirus Pro 2011 测试版或 2008、2009、2010 版本，您可升级到 BitDefender Antivirus Pro 2011。

有两种方法进行升级:

- 直接用 BitDefender Antivirus Pro 2011 覆盖安装老版本。如果您是覆盖安装 2010 版本，隔离区数据会自动导入。
- 卸载老版本，重启电脑，然后按照 “产品安装” （第 5 页）中的指导安装新版本。产品设置将不会被保留。如果另外的升级方式失败，请使用此方法。

5. 修复和卸载BitDefender

如果您要修复或卸载 BitDefender Antivirus Pro 2011，请在 Windows 开始菜单上按以下顺序点击： 开始 → 所有程序 → BitDefender 2011 → 修复或卸载。

会显示一个向导帮助您完成任务。

1. 修复 / 卸载

   选择您希望执行的操作：

   - 修复 – 重新安装所有程序组件。
   - 卸载 – 卸载所有已经安装的组件。

   注意
   我们建议您选择 卸载 以进行一次干净的重装。

2. 确认操作

   请在点击 下一步 确认操作前认真阅读显示的信息。

3. 进度

   请等待 BitDefender 完成您选择的操作。需要花费几分钟时间。

4. 完成

   结果已显示。

   您需要重启电脑以完成此过程。请点击 重启 立即重启电脑，或点击 完成 关闭窗口稍后重启。

开始使用

6. 总揽

在您安装 BitDefender Antivirus Pro 2011 之后，您的电脑就会被保护免受各类恶意软件（如病毒、间谍软件和木马）的侵袭。

除安装时配置的选项外，其他 BitDefender 设置选项不是必须配置的。不过，您也许愿意详细设置 BitDefender 来提高防护。

您应经常打开 BitDefender 并修复存在的问题。您可能需要配置特别的 BitDefender 组件，或者采取预防措施，以保护您的计算机和数据。您也可配置 BitDefender 不向您报告指定的问题。

如果您尚未注册产品（包括创建 BitDefender 账户），请记着在试用期结束前进行注册。您必须在安装BitDefender后15天内创建一个账户（如果您已注册产品，截止日期延长至30天）。否则，BitDefender将不再更新。欲了解更多有关注册过程的信息，请参阅 “注册及我的账号” （第 40 页）。

6.1. 打开 BitDefender

要打开 BitDefender Antivirus Pro 2011 的主界面，请从 Windows 的开始菜单，按以下步骤点击：开始 → 所有程序 → BitDefender 2011 → BitDefender Antivirus Pro 2011，或者采用更快方式，双击 BitDefender 系统托盘图标。

欲了解更多有关程序主窗口的信息，请参见 “程序主窗口” （第 21 页）。

6.2. 系统托盘图标

要想更快捷地管理整个产品，您可以使用 BitDefender 系统托盘图标。如果您双击此图标，BitDefender主界面将会打开。此外，通过右键点击图标，将会显示上下文菜单，从而使您更快捷地管理BitDefender产品。

打开 – 打开Bitdefender主界面。



系统托盘图标

- 帮助 – 打开帮助文件，向您详细介绍如何配置及使用 BitDefender Antivirus Pro 2011。
- 关于 – 打开一个包含Bitdefender及支持信息的窗口。

- 修复全部问题 – 帮您修复当前的安全漏洞。如果选项不可用，则说明没有需要修复的问题。欲了解更多信息，请参阅 “修复问题” （第 33 页）。
- 开启/关闭游戏模式 – 开启或关闭 游戏模式。
- 立即升级 – 立即开始升级产品。将会出现一个新窗口，显示升级状态。
- 偏好设置 – 打开窗口以便您启用或急用主要的产品设置选项或重新配置用户方案。更多信息 请参阅 “配置主要设置” （第 35 页）。

BitDefender 托盘图标通过显示特殊的符号，向您提示影响电脑安全的问题，或者产品的操作行为，如下所示：

带叹号的红色三角: 有严重问题影响您的系统安全，需要您立即关注并尽快解决。
字母 G： 产品处于 游戏模式。

如果 BitDefender 停止工作，系统托盘图标会变灰。这种情况通常在授权密钥过期时发生，此外如果 BitDefender 服务不可用时，或者其他错误影响 BitDefender 的正常操作时，也会发生此情况。

6.3. 扫描活动状态栏

扫描活动条 以图形化方式显示您系统上的扫描活动。这个小窗口默认只在 专家视图 中可用。

灰色条（文件区域） 显示每秒扫描的文件数量，刻度从0到50。



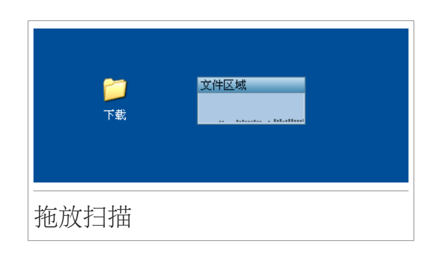
扫描活动状态栏



注意
扫描活动条在实时防护被禁用时会在文件区域上显示一个红叉提醒您。

6.3.1. 扫描文件及文件夹

您可以用扫描活动条快速扫描文件或文件夹。拖动您想扫描的文件或文件夹，将其放到 扫描活动条上，如下图所示。



拖放扫描



放下文件

反病毒扫描向导 将会出现并引导您完成扫描过程。

扫描选项. 扫描选项已经预设，以便取得最好的扫描效果。如果发现了感染的文件，BitDefender 会尝试清除感染的病毒（去掉病毒代码）。如果清除失败，反病毒扫描向导会让您指定针对感染文件的其他操作。扫描选项是标准的，您不能修改它们。

6.3.2. 禁用/恢复扫描活动条

当你不再想查看扫描活动条时，只需右键点击他然后选择 隐藏 即可。要恢复扫描活动条，请按照以下步骤操作：

1. 打开 BitDefender。
2. 点击窗口右上角的 设置 按钮并选择 偏好设置。
3. 在常规设置中，使用对应于 扫描活动条 的开关以启用它。
4. 点击 确定 以保存及应用更改。

6.4. 设备自动检测

当您将一个移动存储设备链接到电脑时，BitDefender 会自动检测到此操作，并可在您访问其中的文件之前对该设备进行扫描。建议选中此项，以阻止病毒及其他恶意软件感染您的电脑。

被检测到的设备分为如下几类：

- CD/DVD
- USB存储设备，如U盘及移动硬盘
- 映射的网络驱动器

当发现这样的设备时，会显示一个警示窗口。

要扫描此存储设备，请点击 是。反病毒扫描向导 将会出现并引导您完成扫描过程。

如果您不想扫描此设置，请选择 否，此时，您可能发现下述选项之一有用：

- 不要再询问我此类设备 - 当此类设备连接到您的电脑时，BitDefender 将不会提示您扫描存储设备。
- 禁用设备自动检测 - 当新设备被连接到电脑时，不会再提醒您。

如果您意外禁用了设备自动检测，并想重新启用此功能，或者当您想重新配置时，请按照下述步骤进行：

1. 打开 BitDefender，点击位于窗口右上角的 设置 并选择 专家视图。
2. 打开 反病毒>病毒扫描。
3. 在扫描任务列表中找到 设备扫描 任务。
4. 右键点击该任务并选择 属性。接着会显示一个新窗口。
5. 在 概览 标签页，按照您的需求配置扫描选项。更多信息 请参阅 “设置扫描选项” （第 60 页）。
6. 在 检测 标签页，选择需要检测的存储设备类型。
7. 点击 确定 以保存及应用更改。

7. 程序主窗口

BitDefender Antivirus Pro 2011 适用于从电脑初学者到电脑专家的所有用户，其用户界面被设计为适合各类用户使用。

您可根据自己的电脑水平以及对 BitDefender 的熟悉情况，从三种视图模式中选择一种用户界面视图。

基本视图
: 适用于电脑初学者及希望 BitDefender 无打扰地保护电脑安全的用户。此模式使用简单，对用户交互的需求最少。

  您所需要做的只是在 BitDefender 发出提示时修复存在的问题即可，BitDefender 会采用直观的向导来引导您一步步解决问题。此外，您还可执行常用任务，如升级或病毒扫描。

中级视图
: 面向一般水平的电脑用户，此界面扩展了基本视图中的内容。

  您可分开处理不同问题，并可以选择监控哪些问题。此外，您还可远程管理您家里其他电脑上的 BitDefender 产品。

专家视图
: 适用于电脑技术高手，此模式下您可全面配置 BitDefender 的各个功能。您可使用 BitDefender 提供的所有功能保护您的电脑和数据。

视图模式在安装过程中被选定。

要更改视图模式：

1. 打开 BitDefender。
2. 点击窗口右上角的 设置 按钮。
3. 请从菜单中选择所需的视图模式。

7.1. 基本视图

如果您是电脑新手，选择“基本视图”的用户界面会比较合适。此模式操作简便，所需的用户交互最少。

此窗口分为三个区域：

状态区
: 状态信息显示在窗口左侧。

“保护您的电脑”区域
: 您可在此选择合适操作管理防护。

帮助区域
: 您可在此了解如何使用 BitDefender Antivirus Pro 2011 并获得帮助。

位于窗口右上角的 设置 按钮可让您修改用户界面视图，以及配置 主要程序设置。

在窗口的右下角，您可看到几个有用的链接。

快捷方式	描述
授权密钥信息	打开窗口，您可看到当前授权密钥信息，并使用新授权密钥注册产品。
查看日志	让您看到BitDefender在您计算机上执行的所有任务的详细历史信息。
帮助及支持	如果您想获得 BitDefender 帮助，请点击此链接。
?	打开帮助文件，让您了解如何使用 BitDefender。

7.1.1. 状态区

状态信息显示在窗口左侧。

- 安全状态 通知您影响电脑安全的问题，并帮您修复问题。点击 修复所有问题，一个向导会帮您轻松修复影响电脑和数据安全的问题。欲了解更多信息，请参阅 “修复问题” （第 33 页）。
- 授权密钥状态 显示授权密钥的有效期。如果您正在使用试用版本，或您的授权密钥即将过期，您可点击 立即购买 购买授权密钥。欲了解更多信息，请参阅 “注册及我的账号” （第 40 页）。

7.1.2. “保护您的电脑” 区域

您可在此选择合适操作管理防护。

有三个按钮可用：

- 安全 提供到安全任务及设置的快捷方式。
- 立即更新 帮助您更新 BitDefender 病毒库及产品文件。将会出现一个新窗口，显示升级状态。如果发现可用更新，会自动下载并且安装到您的电脑中。
- 我的工具 可让您创建到您最常用的功能及设置的快捷方式。

要执行任务或配置选项，请点击对应的按钮并从菜单中选择所需工具。要添加或删除快捷方式，请点击相应按钮并选择 更多选项。欲了解更多信息，请参阅 “我的工具” （第 27 页）。

7.1.3. 帮助区域

您可在此了解如何使用 BitDefender Antivirus Pro 2011 并获得帮助。

智能提示 是了解电脑安全及 BitDefender Antivirus Pro 2011 使用技巧的最佳方式。

如果您需要帮助，请在 帮助及支持 输入框输入关键词或问题，然后点击 搜索。

7.2. 中级视图

中级视图适用于普通电脑水平的用户，交互简单，可以访问所有模块的基本功能。您将需要及时查看产品的警示及严重警告，并修复问题。

中级视图窗口被组织为多个标签。

图表板
: 图表板帮助您方便地监控及管理安全防护。

安全性
: 显示安全设置状态，并帮助您修复发现的问题。您可运行安全任务或配置安全选项。

家庭网络
: 显示Bitdefender家庭网络结构。您可在此针对安装在您家庭网络中的BitDefender 产品进行各种操作，以配置和管理这些产品。这样，您可在一台计算机上管理您家庭网络的安全。

位于窗口右上角的 设置 按钮可让您修改用户界面视图，以及配置 主要程序设置。

在窗口的右下角，您可看到几个有用的链接。

快捷方式	描述
授权密钥信息	打开窗口，您可看到当前授权密钥信息，并使用新授权密钥注册产品。
查看日志	让您看到BitDefender在您计算机上执行的所有任务的详细历史信息。
购买/续订	帮助您购买 BitDefender Antivirus Pro 2011 产品授权密钥。
帮助及支持	如果您想获得 BitDefender 帮助，请点击此链接。
?	打开帮助文件，让您了解如何使用 BitDefender。

7.2.1. 图表板

图表板帮助您方便地监控及管理安全防护。

图表板包含下面的区域:

- 状态详情 使用明确的文字说明各个主要模块的状态，同时使用以下图标之一:

  带对号的绿色圆圈: 暂无影响您系统安全的问题。您的电脑及数据处于保护中。

  带叹号的红色圆圈: 存在影响系统安全的问题。严重问题需要您立即处理，不严重问题也应尽快处理。

- 带叹号的灰色圆圈：本模块各组件的活动未被监测，因此没有关于其安全状态的信息。可能存在与此模块相关的特定问题。

点击模块名称查看其状态的详细信息，并配置该组件的状态追踪设置。

- 授权密钥状态 显示授权密钥的有效期。如果您正在使用试用版本，或您的授权密钥即将过期，您可点击 立即购买 购买授权密钥。欲了解更多信息，请参阅 “注册及我的账号” （第 40 页）。
- 我的工具 可让您创建到您最常用的功能及设置的快捷方式。欲了解更多信息，请参阅 “我的工具” （第 27 页）。
- 智能提示 是了解电脑安全及 BitDefender Antivirus Pro 2011 使用技巧的最佳方式。

7.2.2. 安全性

“安全”标签可帮您管理电脑和数据安全。

“状态区” （第 24 页）
“快速任务” （第 24 页）

状态区

您可在状态区看到所有被监测的安全组件的列表及其当前状态。通过监测安全模块，BitDefender 会在您配置影响系统安全的选项是通知您，并可提醒您忘记执行的重要任务。

每个组件的当前状态使用清晰的语句及下列图标表示：

- 带对号的绿色圆圈： 没有影响此组件的问题。
- 带叹号的红色圆圈： 影响该组件的问题。

点击问题对应的 修复 按钮就可修复该问题。如果问题不能立即解决，请跟随向导的指示来解决。

要配置哪个组件必须被监测：

1. 点击 添加/编辑列表。
2. 要开启或关闭对某个项目的监测，请使用对应的开关。
3. 点击 关闭 已保存修改并关闭窗口。



重要
要确保您的系统被全面防护，请开启针对所有组件的监控，并修复报告的所有问题。

快速任务

您可在这里找到指向重要安全任务的链接：

- 立即升级 – 立即开始升级产品。
- 全面系统扫描 – 开始对系统进行标准扫描(压缩文档除外)。要查看其他手动扫描任务，请点击按钮上的 并选择一个不同的扫描任务。
- 自定义扫描 – 运行一个向导，帮助您创建并运行自定义扫描任务。
- 漏洞扫描 – 启用一个检查系统漏洞并帮您修复漏洞的向导。

7.2.3. 家庭网络

您可在此针对安装在您家庭网络中的 BitDefender 产品进行各种操作，以配置和管理这些产品。这样，您可在一台计算机上管理您家庭网络的安全。

欲了解更多信息，请参阅 “家庭网络” （第 88 页）。

7.3. 专家视图

在专家视图下您可访问 BitDefender 的所有功能组件，在此模式下您可详细设置 BitDefender 的各项功能。



注意
专家视图适合具有较高计算机水平的用户，他们清楚电脑所面临的威胁，以及安全软件如何工作。

在窗口的左侧有一个包含所有安全模块的菜单。每个模块都有一个或多个标签页，您可在其中配置相应的安全设置，或者执行管理任务。下表简要描述了各个模块。欲了解更多信息，请参阅用户手册中的 “配置和管理” （第 43 页）部分。

常规
: 让您访问常规设置选项，或浏览图表板及系统信息。

反病毒
: 您可详细设置您的病毒防护和扫描操作选项，还可以设置扫描白名单和隔离区。您还可在此配置 钓鱼防护 和 搜索建议。

隐私控制
: 防止您的数据被从您的计算机上窃取，并保护您的上网隐私。

漏洞检测
: 让您可以保持您计算机上关键软件处在最新版本。

加密
: 加密您的雅虎通和MSN的通信。

游戏/笔记本模式
: 当您运行在笔记本电池时，推迟bitdefender计划任务；当您在玩游戏时，不显示警告及弹出窗口。

家庭网络
: 让您可以配置及管理家里多台计算机上的BitDefender产品。

更新
: 您可获取最新升级包，升级产品并配置升级过程的细节。

注册
: 允许您注册BitDefender Antivirus Pro 2011，改变许可密钥或建立一个BitDefender帐户。

位于窗口右上角的 设置 按钮可让您修改用户界面视图，以及配置 主要程序设置。

在窗口的右下角，您可看到几个有用的链接。

快捷方式	描述
授权密钥信息	打开窗口，您可看到当前授权密钥信息，并使用新授权密钥注册产品。
查看日志	让您看到BitDefender在您计算机上执行的所有任务的详细历史信息。
购买/续订	帮助您购买 BitDefender Antivirus Pro 2011 产品授权密钥。
帮助及支持	如果您想获得 BitDefender 帮助，请点击此链接。
?	打开帮助文件，让您了解如何使用 BitDefender。

8. 我的工具

当您使用 BitDefender “基本视图” 或 “中级视图” 时，您可自定义图表板，向其中添加重要任务及设置项的快捷方式。这样，您可快速访问经常使用的功能及高级设置，而无需切换到更高级的界面视图。

根据用户界面视图的不同，添加到” 我的工具 “中的快捷方式如下：

基本视图
　　在 “保护您的电脑” 区域，点击 “我的工具” 。您会看到一个菜单。点击快捷方式运行对应的工具。

中级视图
　　快捷方式显示在 “我的工具” 下面。点击快捷方式运行对应的工具。

要打开可以选择显示到 “我的工具” 中的快捷方式的窗口，请参照以下说明：

基本视图
　　在 “保护我的电脑” 区域，点击 “我的工具” 并选择 更多选项。

中级视图
　　点击位于 “我的工具” 下的按钮或点击 配置我的工具 链接。

使用开关选择要添加到 “我的工具” 中的工具。您可任意选择以下分类的工具。

- 扫描任务

添加您常用的扫描任务。

扫描任务	描述
深度系统扫描	扫描整个系统，包括压缩文档。在默认配置下，它扫描威胁到您系统安全的所有类型的恶意软件，如病毒，间谍软件，广告软件， rootkit和其他。
全面系统扫描	扫描整个计算机，不扫描压缩文档。默认配置下，该任务扫描除 rootkits 之外的所有类型恶意软件。
快速扫描	快速扫描使用了云技术检测运行在您电脑中的恶意程序。快速扫描通常少于一分钟，占用的系统资源是普通病毒扫描的很小一部分。
自定义扫描	运行向导，帮助您创建自定义扫描任务。
扫描我的文档	使用这项任务扫描当前用户的重要文件夹：我的文档，桌面 和 启动 。这会确保您的文档和工作环境安全，并保证系统启动时运行的应用程序是安全的。
设置定时扫描	打开反病毒设置窗口，您可在其中自定义手动扫描任务。

欲了解扫描任务的更多信息，请参见 “管理已有扫描任务” （第 57 页）。

- 设定

添加您想配置的 BitDefender 设置项快捷方式：

设定	描述
反病毒设置	配置防病毒模块。欲了解更多信息，请参见 “反病毒防护” （第 48 页）.
游戏模式	切换游戏模式。欲了解更多信息，请参见 “游戏模式” （第 83 页）.
笔记本模式	切换笔记本模式。欲了解更多信息，请参见 “笔记本模式” （第 85 页）.
立即更新	启动 BitDefender 更新。欲了解更多信息，请参见 “更新” （第 91 页）。
查看 & 修复所有问题	打开一个向导，帮您修复所有影响电脑安全的问题。欲了解更多信息，请参见 “修复问题” （第 33 页）.

- 帮助及支持

进入支持区域。欲了解更多信息，请参见 “从 BitDefender 产品直接联系我们” （第 117 页）.

9. 警报和弹出式窗口

BitDefender 使用弹出窗口和警告窗口通知您有关其操作或您需要了解的特殊事件，并提示您在必要时采取行动。本章说明您可能遇到的 BitDefender 弹窗及警告。

弹出式窗口是指临时出现在屏幕上的小窗口，通知您 BitDefender 各种事件，如电子邮件扫描，一个新的计算机登录到您的无线网络，防火墙规则增加等。当弹窗出现时，您最多只需点击 确定 按钮或一个链接。

警告弹窗是较大的窗口，提示您选择操作，或通知您重要信息（如一个病毒已被删除等）。除警告窗口外，您可能还会收到电子邮件、聊天消息及网页形式的警告。

BitDefender 弹窗及警告包括：

- 反病毒警告
- 活动病毒控制警告
- 设备检测警报
- 防钓鱼警告网页
- 隐私控制警告

9.1. 反病毒警告

BitDefender 保护您免费各种恶意软件侵害，如病毒、间谍软件或 Rootkit。检测到病毒或其他恶意软件时，BitDefender 会对感染文件采取指定操作，并通过警告窗口通知您。

您可以看到病毒的名称、受感染文件路径，以及 BitDefender 所采取的操作。

点击 确定 来关闭窗口。



重要

当检测到病毒时，最好对电脑进行全盘扫描以确保没有其他病毒。更多信息 请参阅 “如何扫描文件及文件夹？”（第 95 页）。
如果病毒未被拦截，请参见 “从您的电脑中删除恶意程序”（第 109 页）。

9.2. 活动病毒控制警告

可以配置 AVC 在应用程序试图执行潜在恶意操作时警告您。

如果您正在使用“基本视图”或“中级视图”，每次当活动病毒控制拦截了一个潜在的恶意程序时，您会看到一个弹窗通知。如果您正在使用专家视图，在程序显示出恶意行为时，您会看到一个警告窗口提示您选择操作。

如果您了解并信任所检测到的应用程序，请点击 允许。

如果您想立即关闭该应用程序，请点击确定。

在选择选项之前选中 记住针对此应用程序的操作 复选框，BitDefender 下次会对此程序采取同样操作。创建的规则将会被显示在活动病毒控制配置窗口。

9.3. 设备检测警报

当您将一个移动存储设备链接到电脑时，BitDefender 会自动检测到此操作，并可在您访问其中的文件之前对该设备进行扫描。建议选中此项，以阻止病毒及其他恶意软件感染您的电脑。

被检测到的设备分为如下几类：

- CD/DVD
- USB存储设备，如U盘及移动硬盘
- 映射的网络驱动器

当发现这样的设备时，会显示一个警示窗口。

要扫描此存储设备，请点击 是。病毒扫描向导将会显示，并引导您完成扫描过程。

如果您不想扫描此设置，请选择 否，此时，您可能发现下述选项之一有用：

- 不要再询问我此类设备 - 当此类设备连接到您的电脑时，BitDefender 将不会提示您扫描存储设备。
- 禁用设备自动检测 - 当新设备被连接到电脑时，不会再提醒您。

如果您意外禁用了设备自动检测，并想重新启用此功能，或者当您想重新配置时，请按照下述步骤进行：

1. 打开 BitDefender，点击位于窗口右上角的 设置 并选择 专家视图。
2. 打开 反病毒>病毒扫描。
3. 在扫描任务列表中找到 设备扫描 任务。
4. 右键点击该任务并选择 属性。接着会显示一个新窗口。
5. 在 概览 标签页，按照您的需求配置扫描选项。更多信息 请参阅 “设置扫描选项” （第 60 页）。
6. 在 检测 标签页，选择需要检测的存储设备类型。
7. 点击 确定 以保存及应用更改。

9.4. 反网络钓鱼警报

启用防钓鱼功能后，BitDefender 会在您尝试访问欺诈网站时显示警告。在您可以访问这个网页前，BitDefender 会拦截该网页并会显示一个通用警告网页。

检查您的浏览器地址栏中的网页地址。寻找表明该网页可能是用来网络钓鱼的线索。如果网页地址是可疑的，建议您不要打开它。

这里有一些提示，可能对您有用：

- 如果您键入一个合法网站的地址，检查地址是否正确。 如果地址不正确，重新键入并再次转到网页。

- 如果您已单击了一个电子邮件或即时消息上的链接，请检查是谁发送给您的。 如果发件人是未知的，这就可能是一个网络钓鱼的尝试。 如果您知道发件人，您应该检查这个人是否真的向您发送了链接。
- 如果您已经通过互联网访问了网页，检查您是在哪里发现的这个链接（在您的浏览器上单击返回按钮）。

如果您想要查看网页，单击相应的链接并采取这些操作之一：

- 只本次浏览网页。. 您不在网页上提交任何信息，就不会有风险。如果网页是正常的，您可将其添加到白名单中(点击 BitDefender防钓鱼工具条 并选择 添加到白名单)。
- 添加网页到白名单。. 网页将会立即显示，BitDefender 也不再发出警报。



重要

只有完全值得信赖的网页才可以添加到白名单（例如，银行网址，已知的在线商店等等）。BitDefender 不会检查白名单中网站是否有钓鱼行为。

您可使用网页浏览器中的 BitDefender 工具条来管理钓鱼防护及白名单。更多信息请参阅 “在 IE 和 Firefox 中管理 BitDefender 钓鱼防护” （第 68 页)。

9.5. 隐私控制警告

隐私控制为高级用户提供保护隐私的更多功能。如果您选择启用这几个组件中的任何一个，您将会看到询问您意见的特定警告窗口：

- 注册表控制 - 当应用程序试图修改注册表项以在系统启动时自动执行时，征询您的许可。
- Cookie控制 - 当新网站试图设置Cookie时，征询您的许可。
- 脚本控制 - 当网站试图运行一个脚本或其他活动内容时征询您的许可。

9.5.1. 注册表警报

如果启用注册表控制，当一个新程序视图修改注册表以随 Windows 启动时，您会接到提示，征询您是否允许。

您可看到试图修改Windows注册表的程序名称。



注意

通常在您安装需要在下次系统重启时运行的新软件时，BitDefender 都会警告您。绝大多数情况下，这些程序是合法的，可以被信任。

如果您不清楚该程序，或者该程序看起来可疑，请点击 拦截 防止它修改Windows注册表。否则，请点击 允许 允许修改。

根据您的选择，会创建一条规则并显示在规则表中。以后每当此程序试图修改注册表时，会应用同样的操作选项。

更多信息 请参阅 “注册表控制” （第 75 页）。

9.5.2. 脚本警报

如果启用脚本控制，您在访问运行脚本或其他活动内容的新网站时，会被询问是否允许。

您可看到脚本资源的名称。

点击 是 或 否 就会创建、应用一条规则，并显示在规则表中。当对应网站再次试图运行活动内容时，会自动使用相同操作。



注意

某些网页可能无法正常显示，如果您阻止其活动内容。

更多信息 请参阅 “脚本控制” （第 77 页）。

9.5.3. Cookie 警报

如果启用 Cookie 控制，在新网站试图在您的电脑上设置 Cookie 时，您会被询问是否允许。

您能看到试图设置或发送Cookie文件的程序名。

点击 是 或 否 就会创建、应用一条规则，并显示在规则表中。当您以后连接到网站时，相同的操作会被自动执行。

更多信息 请参阅 “Cookie 控制” （第 75 页）。

10. 修复问题

BitDefender 使用一个问题跟踪系统监测并通知您影响您的电脑安全的问题。默认情况下，该系统会监测一系列非常重要的问题。不过，您可以配置该系统，只选择您希望监测的项目。

这是未解决问题的通知方式:

- 一个特殊符号 会显示在 BitDefender 的 系统托盘 图标上，以表示有待修复问题。此外，如果您将鼠标移动到托盘图标上，还会显示一个气泡窗口提示您存在待解决问题。
- 当您打开 BitDefender 主界面时， “安全状态” 区域会显示影响您系统安全的问题数。
  - 在基本视图中，安全状态显示在窗口左侧。
  - 在 “专家视图” 中，前往 常规 > 图表板 检查安全状态。

10.1. 修复问题向导

修复问题最简便的方法就是按照 修复问题向导 的指示操作。要打开向导，请执行下述操作之一:

- 右键点击 BitDefender 托盘图标 （位于 系统托盘区）并选择 修复全部问题。
- 打开 BitDefender 并根据用户界面视图的不同，参照以下说明继续:
  - 在 “基本视图” 中，点击 查看所有问题。
  - 在” 专家视图 “中，前往 常规 > 图表板 并点击 查看所有问题。



注意
您可添加一个到 我的工具 的快捷方式。

显示电脑上存在的安全威胁列表。

所有当前问题都被选择进行修复。如果有您不想修复的问题，请不选中对应的复选框。清除选择之后，其状态会变成 忽略。



注意
如果您想在指定问题出现时被通知，您需要配置相应的警告系统，参见下一节。

要修复所选的问题，请点击 开始。有些问题会被立即修复，另外一些则会显示一个向导帮您修复。

本向导可帮您修复的问题可分为如下几类:

- 禁用安全设置. 这些问题可通过启用对用的安全设置被立即修复。

- 您需要执行的预防性安全任务. 类似任务正在扫描您的电脑，建议您至少每周扫描一次电脑。通常情况下 BitDefender 会自动为您进行扫描。不过，如果您修改了扫描计划任务，或计划任务未完成，您将会被通知。

  在修复此类问题时，向导会帮助您成功完成任务。

- 系统漏洞. BitDefender 自动检测您系统中的漏洞并警告您。系统漏洞包括下面的内容:

  - Windows 用户账号的弱密码。
  - 电脑中的过期软件。
  - 未安装的 Windows 更新。
  - Windows 自动更新被禁用。

  当这些问题要被修复时，漏洞检测向导会启动。向导会帮助您修复检测到的系统漏洞。欲了解详细信息，请参阅 “检查是否有漏洞” (第 79 页)。

10.2. 配置状态警告

状态警告系统已预先配置好监控您的电脑，并在发现可能影响您的电脑和数据安全问题时警告您。除了默认监测的问题之外，还有一些其他问题可能会警告您。

您可配置警告系统，选择哪些问题需要通知您，从而让警告更符合您的安全需要。您可在 “中级视图” 或 “专家视图” 中完成此操作。

- 在中级模式，警告系统可从单独的位置进行配置。按照下述步骤执行:
  1. 前往 安全 标签。
  2. 点击位于状态区的 添加/编辑列表 链接。
  3. 使用对应于项目的开关修改其警告状态。

- 在专家视图中，警告系统通过一个集中的位置进行设置。按照下述步骤执行:
  1. 前往 常规 > 图表板。
  2. 点击 添加/编辑警告。
  3. 使用对应于项目的开关修改其警告状态。

11. 配置主要设置

您可在偏好设置窗口配置主要的产品设置选项（包括更改用户方案）。要打开窗口，请选择下述操作之一：

- 打开 BitDefender，点击位于窗口右上角的 设置 并选择 偏好设置。
- 右键点击 BitDefender 托盘图标（位于 系统托盘区）并选择 偏好设置。



注意

要详细配置产品选项，请使用“专家视图”界面。欲了解更多信息，请参阅用户手册中的 “配置和管理” （第 43 页）部分。

设置选项分为三组：

- 安全设定
- 警告设置
- 常规设定

要开启或关闭一个设置选项，请使用对应的开关。

要想保存并应用您所做的修改，请点击 确定，要想不保存修改并关闭窗口，请点击 取消。

位于窗口右上角的 重置使用方案 链接可让您重新配置使用方案。更多信息 请参阅 “重新配置使用方案” （第 37 页）。

11.1. 安全设定

您可在此启用/禁用有关电脑和数据安全的多个产品设置选项。要开启或关闭一个设置选项，请使用对应的开关。



警告

请慎重选择禁用实时病毒防护或自动升级。禁用这些功能可能危及计算机的安全。如果您确实需要禁用它们，请记得尽快重新启用。

可用的设置选项有：

反病毒
: 实时防护可确保所有被您或运行于此系统的应用程序所访问的文件已被扫描。

自动更新
: 自动升级可确保最新的 BitDefender 产品及病毒库文件被定时自动下载并安装。更新在默认情况下每小时进行一次。

漏洞扫描
: 自动漏洞扫描警示您系统中的漏洞并提示您修复，以确保系统安全。这些漏洞包括过期软件、强度不高的密码或缺失的 Windows 更新。

反钓鱼
: 反钓鱼功能实时检测欺诈性质的网页并向您发出警示。

搜索建议
: 搜索建议扫描您搜索结果中的链接并通知您哪些安全，哪些不安全。

身份控制
: 个人信息控制帮助您防止个人信息未经您同意被发送到互联网。该功能拦截所有的即时通讯、电子邮件信息及网页内容，阻止您所指定的个人信息被发送到未经授权的接收人（或网址）。

聊天加密
: 即时通讯加密在您的聊天对象也安装了兼容的 BitDefender 产品及通讯软件时，可以保护你们之间通过雅虎通或MSN进行的通话。

这些设置的状态可能会被 BitDefender 问题跟踪系统监测。如果您禁用了监测设置，BitDefender 会提示这是一个需要解决的问题。

如果您不希望您禁用的选项被显示为需要修复的问题，您需要配置问题跟踪系统。您可在中级视图或专家视图中进行配置。欲了解更多信息，请参阅 “配置状态警告”（第 34 页）。

11.2. 警告设置

在此区域，您可关闭 BitDefender 弹窗及警告。BitDefender 使用警告窗口提示您选择操作，使用弹出窗口提示您产品自动采取的操作，以及其他事件。要打开或关闭一类警告，请使用对应的开关。



重要
大部分警告及弹窗应被开启以防止潜在问题。

可用的设置选项有：

反病毒警告
: 反病毒警告在 BitDefender 检测及拦截病毒时通知您。当检测到病毒时，最好对电脑进行全盘扫描以确保没有其他病毒。

活动病毒控制弹出消息
: 如果您正在使用“基本视图”或“中级视图”，每次当活动病毒控制拦截了一个潜在的恶意程序时，您会看到一个弹窗通知。如果您正在使用专家视图，在程序显示出恶意行为时，您会看到一个警告窗口提示您选择操作。

扫描电子邮件弹出消息
: 这些弹窗通知您 BitDefender 正在扫描电子邮件中的恶意程序。

家庭网络管理警告
: 当管理员操作被远程执行时，这些警告会通知用户。

隔离区警告
隔离区警告在较老的隔离区文件被删除时会通知您。

注册弹出消息
注册提醒弹窗提示您需要注册 BitDefender 或通知您授权密钥即将过期或已经过期。

11.3. 常规设定

您可在此启用或禁用影响产品行为及用户体验的设置选项。要开启或关闭一个设置选项，请使用对应的开关。

可用的设置选项有：

游戏模式
游戏模式将临时修改防护设定以降低其在游戏时对您系统性能的影响。

笔记本模式检测
笔记本模式将临时修改防护设定以降低其对您笔记本电池电量的影响。

设定密码
要防止其他人修改 BitDefender 设置选项，请可使用密码保护。当您启用此选项后，您将被提示配置设置选项密码。在输入框中输入所需的密码并点击 确定 以设置密码。

Bitdefender资讯
启用此选项，您将收到来自BitDefender的重要的公司新闻、产品更新或新的安全威胁信息。

产品通知警报
启用此选项，您将收到信息警报。

扫描活动状态栏
扫描活动条是一个小小的透明的窗口，显示 BitDefender 扫描活动的进程。

发送病毒报告
启用此选项，病毒扫描报告将会被发送给Bitdefender实验室进行分析。请注意，这些报告将不包含机密资料，如您的姓名或IP地址，也不会被用作商业用途。

爆发检测
启用此选项，有关潜在病毒爆发的报告会被发送到Bitdefender实验室进行分析。请注意，这些报告将不包含机密资料，如您的姓名或IP地址，也不会被用作商业用途。

11.4. 重新配置使用方案

在安装过程中，您可创建一个使用方案。使用方案反映电脑的主要用途。根据使用方案的不同，产品界面对进行相应的调整以便使您更方便地执行操作。

要重新配置使用方案，请点击 重置使用方案 并参照配置向导的指示。您可使用 下一步 和 上一步 按钮在向导中导航。要退出向导，请点击 取消。

1. 选择您的视图

   选择适合您的用户界面视图。

2. 配置我的工具

   如果您选择了“基本模式”或“中级模式”，可选择您想放置到“图表板”的功能快捷方式。

3. 配置选项

   如果您选择了“专家视图”，请按需配置 BitDefender 设置选项。要开启或关闭一个设置选项，请使用对应的开关。

4. 家庭网络管理

   注意

   此步骤仅当您将“家庭网络管理”添加到“我的工具”时出现。

   您可从下面三个选项中选择一个：

   - 将此电脑设置为“服务器”

     如想通过家庭网络中的其他电脑管理 BitDefender 产品，请选择此选项。

     要加入网络需输入密码。在文本框中输入密码并点击 提交。

   - 设置此电脑为“客户端”

     如果 BitDefender 将会被运行着 BitDefender 的家庭网络中的其他电脑管理，请选择此选项。

     要加入网络需输入密码。在文本框中输入密码并点击 提交。

   - 暂时跳过安装

     选择此选项稍后从 BitDefender 窗口配置此功能。

5. 设置完成

   点击完成。

12. 历史记录及事件

BitDefender 窗口底部的 查看日志 链接会打开一个新窗口，显示 BitDefender 历史记录 & 事件。该窗口向您显示安全相关事件的整体信息。例如，您可以方便地检查升级是否成功执行、是否在计算机上发现恶意软件等。

为了帮助您更好的筛选历史记录及事件，在左侧提供了下面的类别：

- 图表板
- 反病毒
- 隐私控制
- 漏洞检测
- 聊天加密
- 游戏/笔记本模式
- 家庭网络
- 更新
- 注册

可以查看每个类别的事件列表，每个事件都有如下信息：简述、事件发生时 BitDefender 采取的操作，以及事件发生的日期及时间。如果您想了解某个事件更多的信息，请双击该事件。

点击 清除所有日志 将清除过期的老日志，点击 刷新 显示最新的日志。

13. 注册及我的账号

注册有两个步骤:

1. 产品激活（注册 BitDefender 账户）. 您必须创建一个 BitDefender 账户才能接收升级，并获得免费技术支持。如果您已有 BitDefender 账户，请将您的 BitDefender 产品注册到该账户。BitDefender 将会提醒您需要激活产品，并帮您解决这个问题。



重要

您必须在安装 BitDefender 15 天内创建一个账户。否则， BitDefender将不再更新。

2. 使用授权密钥注册. 授权密钥指定您能使用产品的时长。在授权密钥过期后，BitDefender 将停止执行其功能，不再保护您的计算机。您应该在当前授权密钥过期前的几天购买新的授权密钥或续订授权。

如果您在线购买 BitDefender Antivirus Pro 2011 或购买了安装光盘，在安装过程中会提示您使用授权密钥注册产品。

如果您下载 BitDefender Antivirus Pro 2011 试用，您必须使用授权密钥注册产品以在 30 天试用期后仍能继续使用。在试用期间，产品是全功能的，您可测试并了解产品是否满足您的需求。

13.1. 注册BitDefender Antivirus Pro 2011

如果您想使用授权密钥注册产品，或者修改当前的授权密钥，请点击 BitDefender 主界面底部的 授权信息 链接。产品注册窗口将会出现。

您可以看到Bitdefender注册状态，当前的授权密钥以及距离密钥过期所剩天数。

要注册BitDefender Antivirus Pro 2011:

1. 在编辑框中输入授权密钥。



注意

您可以找到您的授权密钥:

- 在光盘标签上。
- 在产品注册卡上。
- 在网上购买的电子邮件中。

如果您没有 BitDefender授权密钥，请点击产品中所提供的链接运行向导购买。

2. 点击 立即注册。
3. 点击完成。

13.2. 激活 BitDefender

要激活 BitDefender，您必须创建或登录 BitDefender 账户。如果您没有在注册向导中注册 BitDefender 账号，请按照如下步骤操作:

基本视图
: 点击 查看所有问题。此向导会帮助您修复所有待修复问题，包括激活产品。

中级视图
: 前往 安全 标签并点击对应产品更新问题的 查看 & 修复 按钮。点击向导窗口中的 开始 以激活产品。

专家视图
: 前往 注册 并点击 激活产品 按钮。

账号注册窗口将会出现。您可在此创建或登录 BitDefender 账号以激活您的产品。

如果您此时并不想创建 BitDefender 账户，请选择 以后创建 并点击 完成。否则，根据您当前的情况继续进行:

- “我没有BitDefender账户” （第 41 页).
- “我已经有一个BitDefender账户” （第 42 页).



重要

您必须在安装 BitDefender 15 天内创建一个账户。否则， BitDefender将不再更新。

我没有BitDefender账户

要成功创建 BitDefender 账户，请遵循下述步骤:

1. 选择 创建新账户。
2. 在对应的输入框中输入所需信息。您在这里提供的信息都将保密。
   - 用户名 – 输入您的电子邮件地址。
   - 密码 – 输入您Bitdefender账户的密码。密码必须在6到16个字符之间。
   - 重输密码 – 再次输入之前指定的密码。

     如果您选择在输入密码时不用密文，则下次就不需重新输入。
   - 密码提示 – 输入一个能帮您回忆起密码的词或短语。

   注意

   账户激活之后，您就可访问 http://myaccount.bitdefender.com 并使用您输入的电子邮件地址和密码登录您的账户。
3. Bitdefender可能会通过您账户的电子邮件地址告知您的特别优惠及促销活动。点击 查看联系人选项 并在出现的窗口中选择一个可用的选项。

- 给我发送所有消息
- 给我发送重要信息
- 不要给我发送任何消息

4. 点击 提交。
5. 点击 完成 关闭窗口。



注意
在使用您的账户之前，您需要激活它。
检查您的电子邮件，并按照 BitDefender 注册服务发给您的邮件中的指示执行操作。

我已经有一个BitDefender账户

Bitdefender会自动检测你这台计算机以前是否注册过Bitdefender账户。在此情况下，请输入您账户的密码并点击 提交。点击 完成 关闭窗口。

如果您已有有效账号，但是 BitDefender 没有检测到，请参照下述步骤将产品注册到该账号：

1. 选择 登录(已有账户)。
2. 输入您账号的电子邮件和密码。



注意
如果您忘记了密码，请点击忘记密码?然后按照说明进行。

3. Bitdefender可能会通过您账户的电子邮件地址告知您的特别优惠及促销活动。点击 查看联系人选项 并在出现的窗口中选择一个可用的选项。
   - 给我发送所有消息
   - 给我发送重要信息
   - 不要给我发送任何消息
4. 点击 提交。
5. 点击 完成 关闭窗口。

13.3. 购买或续订授权密钥

如果试用期很快就要结束，您必须购买一个授权密钥并注册您的产品。

同样，如果您当前的授权莫要即将过期，您需要续订您的授权密钥。作为 BitDefender 用户，您在续订 BitDefender 授权时可以获得优惠折扣。您还可以特惠折扣或免费将您的产品升级到最新版。

要购买新授权密钥或更新现有密钥，请在“中级视图”中打开 BitDefender 并点击位于窗口底部的 购买 / 续订 链接。

配置和管理

14. 常规设定

常规模块显示BitDefender活动信息及您计算机的系统信息。您也可在此修改BitDefender的常规设置。

要配置通用选项:

1. 打开 BitDefender，点击位于窗口右上角的 设置 并选择 专家视图。
2. 前往 常规 > 设置。

- 为设置操作启用密码保护 – 设定一个密码，以保护BitDefender设置选项不被无权限的人修改。



注意
如果您不只是个人有管理员权限使用这台计算机，建议用密码保护您的BitDefender设置。

在 密码 输入框输入密码，在 再次输入密码 输入框再输入一遍，然后点击 确定。

一旦您设置了密码，您将被要求输入密码才能更改BitDefender设置。其他的系统管理员（如果有的话）也必须提供这个密码才能修改Bitdefender设置。



重要
如果您忘记了密码，您必须修复产品以修改BitDefender设置。

- 显示BitDefender资讯（安全相关通知） – 不定期显示由BitDefender服务器发送的病毒爆发通知。
- 在显示弹出消息（屏幕显示） – 显示产品状态相关的弹出窗口。您可设置让BitDefender 仅在 “基本视图” 、 “中级视图” 或 “专家视图” 中显示弹出窗口。
- 启用扫描活动条(屏显的产品活动图) – 在您登录到 Windows时显示 扫描活动。如果您不想扫描活动条被显示，清除这个复选框。



注意
这个选项只可配置给当前Windows用户账户。扫描活动条仅在界面处于专家视图时可见。

病毒报告设定

- 发送病毒报告 – 把在您的计算机发现的病毒报告递交给BitDefender实验室，这有助于我们掌握和追踪病毒的爆发。

  该报告将不包含机密数据，例如您的名字，IP地址或其它资料。 也不会用于商业目的。 提供的信息只包含病毒名称，将完全用于建立统计报告。

- 启用病毒爆发报告 - 将潜在的病毒爆发报告发送给BitDefender实验室。

  该报告将不含有机密数据，例如您的名字，IP地址或其它资料。 也不会用于商业目的。 提供的信息只包括病毒名称，将完全用于侦测新的病毒。

连接设置

多个 BitDefender 模块（如防火墙、自动更新、实时病毒报告及实时垃圾邮件报告等）需要连接互联网。BitDefender 包含一个代理服务器管理工具以方便您几种管理供 BitDefender 组件上网使用的代理服务器设置。

如果您的公司使用代理服务器连接到互联网，您必须要指定代理服务器设置，以便BitDefender进行更新。否则，它将使用管理员安装产品时设置的代理设置或当前用户的默认浏览器的代理设置(如果有的话)。更多信息 请参阅 “如何找到我的代理服务器设置？”（第 123 页）。



注意
只有具有系统管理员权限的用户或超级用户（知道产品配置密码的用户）才能修改代理服务器设置。

要管理代理服务器设置，请点击 代理服务器设置。

代理服务器设置分为三组：

- 安装时检测到的代理服务器 - 在使用管理员帐户登录并安装本产品时检测到的代理服务器设置，只有当您用管理员帐户登录时才可以进行配置。如果代理服务器需要输入用户名和密码，您必须在对应的输入框中输入。
- 默认浏览器代理服务器 - 从默认浏览器中获取的当前用户代理服务器设置。如果代理服务器需要用户名和密码，您必须在相应的输入框中输入。



注意
支持的浏览器为Internet Explorer、Mozilla Firefox 和 Opera。如果您使用其他浏览器，BitDefender 将无法获取当前用户的代理服务器设置。

- 自定义代理服务器 - 如果您是以系统管理员登录，您可以配置自定义的代理服务器设置。

  需要指定如下设置选项：
  - 地址 - 输入代理服务器IP地址。
  - 端口 - 输入代理服务器端口。
  - 用户名 - 输入代理服务器用户名。
  - 密码 - 输入以上指定用户名的密码。

BitDefender 将根据以下顺序使用代理服务器设置，直到连接到互联网：

1. 指定的代理服务器设置。
2. 安装时检测到的代理服务器设置。
3. 当前用户的代理服务器设置。

在试图连接到互联网时，BitDefender会尝试每一组代理服务器设置，直到连接成功。

首先会尝试您自己的代理服务器设置，如果连接不成功，则会尝试安装时检测的管理员代理服务器设置，如果还不能成功，则会尝试从默认浏览器中检测到的当前用户代理服务器设置。

点击 确定 保存修改并关闭窗口。

点击 应用 保存更改或点击 默认 加载默认设置。

系统信息

BitDefender可以让您从一个单一位置查看所有的系统设置和注册在Windows启动运行时的应用程序。这样，您可以监控系统的活动和安装的应用程序以及找出可能的系统感染。

要获取系统信息:

1. 打开 BitDefender，点击位于窗口右上角的 设置 并选择 专家视图。
2. 前往 常规 > 系统信息。

列表包含所有在系统启动时自动加载的项目，以及有各个应用程序加载的项目。

有三个按钮可用:

- 恢复 – 将当前的文件关联恢复到默认值。仅适用 文件关联 设置!
- 转到 – 打开一个窗口，显示所选的项目（例如 注册表）。



注意
根据所选项目的不同，转到 按钮不一定出现。

- 刷新 – 重新打开 系统信息 部分。

优化

“优化”标签在您您希望执行手动扫描，而不打扰工作时非常有用。

例如，您想运行深度系统扫描，同时硬盘上有大量文件，或系统配置未达到推荐要求，就可能会花较多时间。

要访问“优化”标签页:

1. 打开 BitDefender，点击位于窗口右上角的 设置 并选择 专家视图。
2. 前往 常规 > 优化。

系统负载会被持续监控。当系统空闲时，BitDefender 可以启动:

- 深度系统扫描

- 快速扫描
- 全面系统扫描
- 扫描我的文档



注意
选择 运行任务前更新产品 check 复选框以确保您有最新的病毒特征数据。

15. 反病毒防护

Bitdefender保护您的电脑免受各类的恶意软件侵害（如病毒、木马、间谍软件、rootkit等）。BitDefender病毒保护分为两类:

- 实时防护 – 防止新的恶意软件威胁进入您的系统。举例来说，Bitdefender会在您打开一个Word文档时扫描其中是否存在病毒，或者在您接受电子邮件时对其进行扫描。

  实时保护也被称为访问时扫描 – 文件在用户访问时被扫描。



重要
为防止病毒感染您的计算机，请保持启用 实时防护。

- 请求式扫描 – 检测并清除系统中已经存在的恶意软件。这是由用户启动的传统扫描方式 – 用户选择要扫描的磁盘、文件夹，BitDefender按照用户的需求进行扫描。扫描任务允许您创建自定义的扫描例程，并按时间表定期执行。

在检测到病毒或其他恶意软件时，BitDefender 会自动尝试清除恶意代码，将文件恢复到原始状态。此操作被称为“清除”。无法清除的文件会被移动到隔离区以隔离感染。更多信息 请参阅 “隔离区” （第 66 页）。

如果电脑已感染病毒，请参见 “从您的电脑中删除恶意程序” （第 109 页）。

高级用户可为不希望被扫描的文件配置扫描例外。更多信息 请参阅 “配置扫描排除” （第 63 页）。

15.1. 实时防护

BitDefender扫描所有被访问的文件、电子邮件消息和即时通讯流量，为您提供连续的实时防护，保证系统远离恶意软件。

默认的实时防护设置确保针对恶意软件的良好保护，同时对系统性能影响极小。只需切换到预定义的几个防护级别，您就可方便地根据您的需要设置实时防护选项。如果您是高级用户，您可通过创建自定义防护级别详细配置扫描选项。

欲了解更多信息，请参加这些主题:

- “调整实时防护级别” （第 49 页）
- “创建自定义防护级别” （第 49 页）
- “修改对检测出文件的操作” （第 50 页）
- “恢复默认设置” （第 51 页）

为保护您免受未知恶意程序侵害，BitDefender 使用一种高级启发技术(活动病毒控制Active Virus Control) 及一种入侵检测系统持续监控您的电脑系统。欲了解更多信息，请参加这些主题:

- “配置活动病毒控制” （第 51 页）
- “配置入侵检测系统” （第 53 页）

15.1.1. 调整实时防护级别

实时防护级别定义实时防护扫描选项。只需切换到预定义的几个防护级别，您就可方便地根据您的需要设置实时防护选项。

要调整实时防护级别：

1. 打开 BitDefender。
2. 根据您所使用的用户界面视图模式不同，参照下述说明继续：

   中级视图
      前往 安全 标签并点击窗口左侧 “快速扫描” 区域的 配置反病毒。

      前往 防护 标签。

   专家视图
      前往 反病毒 > 防护。



注意

在 “基本视图” 和 “中级视图” ，您可配置快捷方式以便从图表板访问这些设置。更多信息 请参阅 “我的工具” （第 27 页）。

3. 拖动滑杆设置合适的防护级别。参考滑动条右侧的描述选择适合您安全需求的防护级别。

15.1.2. 创建自定义防护级别

高级用户可以利用BitDefender提供扫描设置。该扫描程序可设置为只扫描特定文件扩展名，搜索特定的恶意软件威胁或跳过存档。这可能会大大减少扫描时间，提高您的电脑在扫描时的反应。

您可创建一个自定义防护级别以详细配置实时防护选项。要创建自定义防护级别：

1. 打开 BitDefender，点击位于窗口右上角的 设置 并选择 专家视图。
2. 前往 反病毒 > 防护。
3. 点击 自定义级别。
4. 按您所需配置扫描选项。想了解某个选项的具体含义，将鼠标放在该选项上面，在窗口底部就会显示描述。
5. 点击 确定 保存修改并关闭窗口。

您可能会发现此信息有用：

- 如果您对某些词汇不熟悉，请在 术语表 中点击它。您也可在互联网上搜索相关信息。
- 扫描访问的文件. 您可设置 BitDefender 扫描所有被访问的文件、仅扫描程序文件或仅扫描您认为危险的特定文件类型。扫描所有被访问的文件可提供最佳防护，而仅扫描程序文件建议在需要更佳系统性能时使用。

  程序文件比其他类型文件更易遭到恶意程序攻击。此类别包括以下文件扩展名：.exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml; .nws.

  如果您选择 扫描用户定义的文件扩展名，建议您包括除您认为危险的文件扩展名外的所有程序扩展名。
- 只扫描新文件及修改过的文件. 只扫描新文件及修改过的文件可极大提升系统相应速度，同时牺牲极少一点安全性。
- 扫描压缩包内容. 扫描压缩文件内部不但耗时长，而且占用系统资源较多，因此不建议在实时防护时扫描压缩文件。包含感染文件的压缩文档不会对您的电脑安全立即造成威胁。只有当恶意程序被从压缩文件中解压出来，而且在实时防护未开启时运行，才会对电脑造成破坏。
- 操作选项. 如果您想修改对检测到的文件的操作，请查看提示于 “修改对检测出文件的操作” （第 50 页）。
- 电子邮件、网页及网络聊天消息扫描选项. 要防止恶意软件下载到您的电脑，BitDefender 自动扫描以下恶意软件入侵点：
  - 收到的电子邮件
  - 网页流量
  - 通过雅虎通及 MSN 收到的文件

  扫描上网流量可能会稍微增加网页加载时间，但是这样做会拦截网页挂马和下载恶意软件。

  虽然不建议，但是您可以禁用对电子邮件、网页及聊天信息的病毒扫描，以提升系统性能。如果您禁用了相应的扫描选项，来自互联网的电子邮件及文件将不会被扫描，可能会导致被感染文件存放到您的电脑中。这不是一个严重威胁，因为实时防护会在文件被访问（如打开、移动、复制或执行）时拦截恶意程序。

15.1.3. 修改对检测出文件的操作

实时防护检测出的文件被分为两类：

- 被感染的文件. 被检测为感染的文件匹配上了 BitDefender 病毒库中的一个特征。BitDefender 通常可以从被感染的文件中删除掉恶意代码，将文件恢复到原始状态。这个操作被称作“清除”。



注意
病毒特征是从真实恶意程序中提取的代码片段，由反病毒程序用来执行模式匹配以检测恶意程序。
BitDefender病毒特征库是由 BitDefender 恶意软徐分析师每小时更新的恶意软件特征集合。

- 可疑文件. 文件被启发式分析引擎检测为可疑。可以文件无法被清除，因为没有可用清除例程。

根据检测出的文件类型不同，会自动采取以下操作:

- 如果检测到感染文件，BitDefender 将会自动尝试清除感染。如果清除病毒失败，文件会被移动到隔离区以隔离病毒。



重要
对于特殊类型的恶意软件，由于整个程序都是恶意代码，因此无法做清除处理。此时，恶意文件会被从磁盘上删除。

- 如果检测到可疑文件，文件会被禁止访问以防止潜在感染。

除非有很强的理由，否则您不应修改针对检测到的文件的默认操作。

要修改对感染及可疑文件的默认操作:

1. 打开 BitDefender，点击位于窗口右上角的 设置 并选择 专家视图。
2. 前往 反病毒 > 防护。
3. 点击 自定义级别。
4. 根据需要为每类检测到的文件配置要采取的操作。如果首选操作失败，备选操作会被执行（比如，如果不可清除，感染文件会被移动到隔离区）。

15.1.4. 恢复默认设置

默认的实时防护设置确保针对恶意软件的良好保护，同时对系统性能影响极小。

要恢复默认的实时防护设置:

1. 打开 BitDefender，点击位于窗口右上角的 设置 并选择 专家视图。
2. 前往 反病毒 > 防护。
3. 点击 默认级别。

15.1.5. 配置活动病毒控制

BitDefender 活动病毒控制根据程序行为检测潜在有害程序。

活动病毒控制持续监测电脑中运行的程序，查看其是否有恶意行为。每个行为都被评分并会按程序计算总分。当进程的总评分超过阈值后，该进程就会被认定为有害。根据程序设置不同，进程会被自动阻止，或提示您选择一个操作。

可以配置 AVC 在应用程序试图执行潜在恶意操作时警告您。

如果您了解并信任所检测到的应用程序，请点击 允许。

如果您想立即关闭该应用程序，请点击确定。

在选择选项之前选中 记住针对此应用程序的操作 复选框，BitDefender 下次会对此程序采取同样操作。创建的规则将会被显示在活动病毒控制配置窗口。

要配置活动病毒控制：

1. 打开 BitDefender，点击位于窗口右上角的 设置 并选择 专家视图。
2. 前往 反病毒 > 防护。
3. 点击 高级设置。
4. 前往 活动病毒控制 标签。
5. 请选择对应的复选框启用活动病毒控制。
6. 拖动滑杆设置合适的防护级别。参考滑动条右侧的描述选择适合您安全需求的防护级别。

调整级别

要配置活动病毒控制防护级别：

1. 打开 BitDefender，点击位于窗口右上角的 设置 并选择 专家视图。
2. 前往 反病毒 > 防护。
3. 点击 高级设置。
4. 前往 活动病毒控制 标签。
5. 拖动滑杆设置合适的防护级别。参考滑动条右侧的描述选择适合您安全需求的防护级别。

配置对恶意行为的响应

如果一个程序表现出恶意行为，您会被询问允许或阻止它。

要配置对恶意行为的响应：

1. 打开 BitDefender，点击位于窗口右上角的 设置 并选择 专家视图。
2. 前往 反病毒 > 防护。
3. 点击 高级设置。
4. 前往 活动病毒控制 标签。
5. 如果您希望在活动病毒控制发现潜在有害程序时被询问处理方式，请选择 采取操作前询问我 复选框。要自动阻止显示出恶意行为的程序（不显示警告窗口），请清除此复选框。

管理信任/不信任程序

您可将自己了解并信任的程序加入信任程序列表，这些程序将不会被 BitDefender 活动病毒控制检查，并被自动允许访问。

要管理不被活动病毒控制模块监控的程序：

1. 打开 BitDefender，点击位于窗口右上角的 设置 并选择 专家视图。
2. 前往 反病毒 > 防护。
3. 点击 高级设置。
4. 前往 活动病毒控制 标签。
5. 点击 排除 标签。

您已为其创建规则的程序会显示在 排除列表 表格中。每条规则对应程序的路径及您所选择的操作(允许或阻止)都会被显示。

要修改针对一个应用程序的操作，请点击当前操作并从菜单中选择其他操作。

要管理列表，请使用表格上方的按钮：

- 添加 – 向名单中加入一个新应用程序。
- 删除 – 从列表中删除一个程序。
- 编辑 – 修改应用程序的规则。

15.1.6. 配置入侵检测系统

BitDefender 入侵检测系统监测网络及系统活动，以发现恶意行为或违规行为。

要配置入侵检测系统：

1. 打开 BitDefender，点击位于窗口右上角的 设置 并选择 专家视图。
2. 前往 反病毒 > 防护。
3. 点击 高级设置。
4. 前往 入侵检测系统 标签。
5. 选择对应的复选框以启用入侵检测系统。
6. 拖动滑杆设置合适的级别。参考滑动条右侧的描述选择适合您安全需求的防护级别。

15.2. 手动扫描

BitDefender的主要目标是使您的计算机不受病毒侵害。这首先是通过排除新病毒入侵您的计算机和扫描您的电子邮件信息，任何新的文件下载或复制到您的系统。

在您安装BitDefender之前，有可能病毒已经存在于您的系统。因此最好在您安装BitDefender后，立即扫描您的计算机。经常扫描计算机检查病毒是一个良好的习惯。

手动扫描基于系统扫描任务，扫描任务指定扫描的选项以及需要扫描的对象。您可以随时运行默认的扫描任务或者您自定义的扫描任务扫描您的计算机，您还可为扫描任务设置运行计划，以便定时运行扫描任务或者在系统空闲时运行。要查看快速指南，请参见这些主题:

- “如何扫描文件及文件夹？” （第 95 页）
- “如何创建自定义扫描任务？” （第 97 页）
- “如何设置定时扫描？” （第 98 页）

15.2.1. 扫描文件和文件夹

任何时候当您怀疑文件或文件夹被感染时，您应尽快对其进行扫描。右键点击您想扫描的文件或文件夹并选择 使用BitDefender扫描。反病毒扫描向导 将会出现并引导您完成扫描过程。

如果您想扫描电脑上的指定位置，您可配置并运行一个自定义扫描任务。更多信息请参阅 “如何创建自定义扫描任务？” （第 97 页）。

要全部或部分扫描您的计算机，您可运行默认的扫描任务或您自己创建的任务。要运行扫描任务，请打开 BitDefender 并根据用户视图的不同选择如下操作:

基本视图
: 点击 安全 按钮并选择可用扫描任务之一。

中级视图
: 前往 安全 标签。点击位于左侧“快速任务”区域的 全面系统扫描 并选择可用的扫描任务之一。

专家视图
: 前往 反病毒 > 病毒扫描。要运行系统或用户定义的扫描任务，请点击相应的 运行任务 按钮。

这是您可用来扫描电脑的默认任务:

全面系统扫描
: 扫描整个计算机，不扫描压缩文档。默认配置下，该任务扫描除 rootkits 之外的所有类型恶意软件。

快速扫描
: 快速扫描使用了云技术检测运行在您电脑中的恶意程序。快速扫描通常少于一分钟，占用的系统资源是普通病毒扫描的很小一部分。

深度系统扫描
: 扫描整个系统，包括压缩文档。在默认配置下，它扫描威胁到您系统安全的所有类型的恶意软件，如病毒，间谍软件，广告软件， rootkit和其他。

在您运行扫描任务之前。请确保Bitdefender已升级到最新的病毒库。用过时的病毒库扫描您的计算机可能会漏掉上次升级后发现的最新恶意软件。

为了能让BitDefender进行完整的扫描，您必须关闭所有的程序。尤其是您的电子邮件客户端(如Outlook，Outlook Express 或 Eudora)必须关闭。

扫描小技巧

扫描小技巧大放送：

- 根据您硬盘大小的不同，运行一次完整的扫描（如深度系统扫描或系统扫描）可能会花相当长时间（一小时以上）。因此，您应该在计算机有较长空闲时间的时候运行这样的扫描。

  您可以 设置扫描计划任务 以便在合适的时间开始扫描。请确保您离开时电脑在运行。在 Windows Vista下，请确保在执行计划任务时，您的计算机未处于休眠模式。

- 如果您经常从互联网上向一个目录下载文件，您可以创建一个扫描任务并 将该目录设置为扫描目标。同时设置此任务每天或更高频度运行。
- 有些病毒会通过修改Windows设置，使得自身在系统启动时运行。要保护您的电脑免受此类恶意软件侵扰，您可以为 自动登录扫描 设置计划任务，在开启启动时运行此任务。请注意自动登录扫描可能在启动后短时间影响系统性能。

15.2.2. 反病毒扫描向导

当您启动一个手动扫描时（比如在文件夹上点击右键并选择使用 BitDefender 扫描）时，BitDefender 反病毒扫描向导将会出现。请遵循向导程序的三个步骤来完成扫描过程。



注意

如果扫描向导未出现，可能是因为扫描被配置为在后台静默运行。您将看到 扫描进程体表出现在 系统托盘。您可以点击此图标打开扫描窗口，查看扫描进度。

步骤 1/3 — 正在扫描

Bitdefender将开始扫描选定的对象。

您可以看到扫描的状态和统计(扫描速度，消耗时间，扫描/感染/可疑/隐藏对象的数量及其他)。

请等待Bitdefender完成扫描。



注意

扫描过程可能需要较长时间，取决于扫描的复杂程度。

密码保护的文档. 如果检测到了密码保护的文档，根据扫描选项不同，您可能会被提示输入密码。有密码保护的档案不能被扫描，除非您提供密码。您可做以下选择:

- 我想为此对象输入密码. 如果您希望 BitDefender 扫描该文档，请选择此选项并输入密码。如果您不知道密码，请选择其他选项之一。
- 我不想为此对象输入密码（跳过此对象）. 选择此选项以跳过扫描该文档。
- 我不想为任何对象输入密码（跳过所有密码保护的对象）. 如果您不想处理密码保护的文档，请选择此项。BitDefender 将不能扫描这些文档，但是会在日志中写入一条记录。

点击 确定 继续扫描。

停止或暂停扫描. 可以在任何时候停止扫描，点击 停止&是. 您将直接跳到向导的最后一步。要暂停扫描，只要点击 暂停 ，您需要点击 继续 恢复扫描。

步骤 2/3 — 选择操作

当扫描完成后，一个新的窗口将出现，就您可以看到扫描的结果。

如果没有为解决的威胁，请点击 继续。否则，您必须为未解决的问题配置新操作，以保护您的电脑。

被感染的对象根据它们所感染的病毒分组显示。点击对应某个病毒的链接，可以看到感染对象的更多信息。

您可以为所有的文件选择一个统一的操作，也可单独为每组文件单独选择操作。以下选项中的一个或多个会出现在菜单中:

不采取任何操作
: 已处理检测出的文件。在扫描完成后，您可以打开扫描日志查看这些压缩文档的信息。

清除病毒
: 从感染文件中移除恶意代码。

删除文件
: 从磁盘上删除检测出的文件。

移动至隔离区
: 移动受感染文件到隔离区。被隔离的文件将不能被执行或打开，因此不存在感染其他文件的风险。更多信息 请参阅 “隔离区” （第 66 页）。

重命名名称
: 通过追加 .bd.ren 在他们的名称后面更改隐藏文件的名称。因此，您将能够在您的计算机上搜索和找到这些文件。

  请注意这些隐藏文件并非您故意在Windows中设置隐藏的，这些文件是由特殊的程序隐藏的，通常称为 rootkit。Rootkit 本质上并非恶意，但是它们常被用来防止反病毒软件检测出病毒或间谍软件。

点击 继续 执行所选的操作。

步骤 3/3 — 查看结果

当BitDefender完成处理检测出的问题后，将会在一个新窗口显示扫描结果。如果您想了解扫描过程的完整信息，请点击 查看日志 浏览扫描日志。



重要
如有需要，请重新启动系统以完成清除过程。

点击 关闭 关闭窗口。

Bitdefender未能解决部分问题

在大多数情况下，Bitdefender能成功清除受感染的文件或隔离受感染的文件。不过，有些问题无法被自动解决。欲了解手动删除恶意软件的更多信息，请参见 “从您的电脑中删除恶意程序” （第 109 页）。

Bitdefender检测到可疑文件

可疑文件是被启发式分析程序检测为可能感染了未知的病毒特征码。

如果在扫描期间发现可疑文件，您会被要求提交给BitDefender实验室。点击 确认 发送这些文件给Bitdefender实验室进行分析。

15.2.3. 查看扫描日志

每次运行扫描时，都会创建一份扫描日志。扫描日志包含扫描过程的详细信息，如扫描选项、扫描对象、发现的病毒，以及针对各个文件采取的操作等。

在扫描完成后，您可点击 查看日志 从扫描向导中直接打开扫描日志。

要稍后再查看扫描日志:

1. 打开 BitDefender。
2. 点击窗口右下角的 查看日志 链接。
3. 点击左侧菜单的 反病毒。
4. 在 手动扫描任务 区域，您可了解最近进行了什么扫描。双击列表中的事件查看更多信息。要打开扫描日志，请点击 查看扫描日志。扫描日志会在默认浏览器中打开。

要删除一个日志项，右键单击它并选择 删除。

15.2.4. 管理已有扫描任务

BitDefender自带有几个默认的任务，其中包括共同的安全问题。您也可以创建您自己定制的扫描任务。更多信息 请参阅 “如何创建自定义扫描任务？” （第 97 页）。

要管理已有的扫描任务:

1. 打开 BitDefender。
2. 根据您所使用的用户界面视图模式不同，参照下述说明继续：

中级视图
: 前往 安全 标签并点击窗口左侧 “快速扫描” 区域的 配置反病毒。

前往 病毒扫描 标签。

专家视图
: 前往 反病毒 > 病毒扫描。



注意

在 “基本视图” 和 “中级视图” ，您可配置快捷方式以便从图表板访问这些设置。更多信息 请参阅 “我的工具” （第 27 页）。

有3种类别的扫描任务：

- 系统扫描任务 – 包含以下默认的系统扫描任务：

全面系统扫描
: 扫描整个计算机，不扫描压缩文档。默认配置下，该任务扫描除 rootkits 之外的所有类型恶意软件。

快速扫描
: 快速扫描使用了云技术检测运行在您电脑中的恶意程序。快速扫描通常少于一分钟，占用的系统资源是普通病毒扫描的很小一部分。

自动登录扫描
: 扫描当用户登录到Windows操作系统时被运行的项目。默认情况下，自动登录扫描被禁用。

如果您想使用这项任务，请用右键点击它，选择 任务计划 并设置任务在 系统启动时运行。您可以指定在系统启动后多长时间运行此扫描任务。

深度系统扫描
: 扫描整个系统，包括压缩文档。在默认配置下，它扫描威胁到您系统安全的所有类型的恶意软件，如病毒，间谍软件，广告软件， rootkit和其他。



注意

因为 深度扫描和完全扫描 任务分析整个系统，扫描可能需要持续一段时间。因此，我们建议您以低优先级方式运行这些任务，最好是在系统空闲的时候。

- 用户扫描任务 包含用户自定义的扫描任务。

默认提供了一个名为 扫描我的文档的任务。使用这项任务扫描当前用户的重要文件夹：我的文档，桌面 和 启动 。这会确保您的文档和工作环境安全，并保证系统启动时运行的应用程序是安全的。

- 其他扫描任务 —包含多个其他扫描任务，这些任务比较独特，不能从本窗口启动。您只能修改这些任务的设置，或查看扫描报告。以下任务可用：

  设备扫描中
  : BitDefender 能自动检测连接到电脑的新存储设备并对其进行扫描。使用该操作配置存储设备（CD/DVD，USB 存储设备或映射网络驱动器）的自动检测和扫描选项。

  右键菜单扫描
  : 当通过 Windows 右键菜单扫描或使用 扫描活动条 扫描时使用此任务。您可以更改扫描选项，使其更好地满足您的需要。

您可使用按钮及快捷菜单管理扫描任务。

要运行系统或用户定义的扫描任务，请点击相应的 运行任务 按钮。反病毒扫描向导 将会出现并引导您完成扫描过程。

要设置一个扫描任务定时运行，请点击相应的 计划任务 按钮并按您所需配置运行时间。

如果您不再需要一个之前创建的扫描任务，可点击位于该任务右侧的 删除 按钮进行删除。您不能删除系统或杂项任务。

每个扫描任务都有一个“属性”窗口，您可在其中配置扫描选项并查看扫描日志。要打开此窗口，请点击任务名称左侧的 属性 按钮，或者右键点击该任务并选择 属性。

欲了解更多信息，请参加这些主题：

- “设置扫描选项”（第 60 页）
- “设置扫描对象”（第 62 页）
- “设置扫描任务运行计划”（第 62 页）

快捷菜单

每个扫描任务都有快捷菜单，在任务上单击鼠标右键就可打开快捷菜单。

对于系统及用户定义扫描任务，在快捷菜单上会显示如下的命令：

- 立即扫描 – 运行选定的扫描任务，启用即时扫描。
- 路径 – 打开 属性 窗口的 路径 标签页，您可在此修改选定任务的扫描对象。在系统任务中，此选项会被替换为 显示扫描路径，因为您只能查看其扫描的对象。
- 任务计划 – 打开 属性 窗口的 任务计划 标签页，您可在此为选定的任务设置运行计划。
- 查看日志 – 打开 属性 窗口， 日志 标签页，您可在此看到选中任务运行后产生的报告。

- 复制任务 - 复制指定的扫描任务。这在建立新任务时非常有用，因为您可通过复制并修改已有的扫描任务快速创建一个新任务。
- 删除 - 删除指定的扫描任务。



注意
仅对用户创建的任务可用，您无法删除默认任务。

- 属性 - 打开 属性 窗口， 浏览 页签，在那里您可以改变选定任务的配置。

由于 杂项任务 类别的特殊性，只有 查看日志 和 属性 两个选项可用。

设置扫描选项

要为某个扫描任务设置扫描选项，请右键点击该任务，并选择 属性。

您可方便地通过调整扫描级别来配置扫描选项，只需拖动滑块就可调整扫描级别。参考滑动条右侧的描述选择适合您安全需求的扫描级别。

您也可配置这些通用选项：

- 以低优先级运行任务. 调低扫描过程的优先级，这将让其他程序运行速度更快，并增加扫描进程完成的时间。
- 最小化扫描向导到系统托盘. 将扫描窗口最小化到 系统托盘，双击BitDefender系统托盘图标可以打开窗口。
- 指定没有发现威胁时的操作。

高级用户可以利用BitDefender提供扫描设置。该扫描程序可设置为只扫描特定文件扩展名，搜索特定的恶意软件威胁或跳过存档。这可能会大大减少扫描时间，提高您的电脑在扫描时的反应。

要详细配置扫描选项：

1. 点击 自定义。
2. 按您所需配置扫描选项。想了解某个选项的具体含义，将鼠标放在该选项上面，在窗口底部就会显示描述。
3. 点击 确定 保存修改并关闭窗口。

您可能会发现此信息有用：

- 如果您对某些词汇不熟悉，请在 术语表 中点击它。您也可在互联网上搜索相关信息。
- 扫描级别. 选择适当的选项指定您希望 BitDefender 扫描的恶意软件类型。
- 扫描文件. 您可设置 BitDefender 扫描所有被访问的文件、仅扫描程序文件或仅扫描您认为危险的特定文件类型。扫描所有文件提供最佳防护，而仅扫描程序文件只建议用作快速扫描。

程序文件比其他类型文件更易遭到恶意程序攻击。此类别包括以下文件扩展名：.exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml; .nws.

如果您选择 扫描用户定义的文件扩展名，建议您包括除您认为危险的文件扩展名外的所有程序扩展名。

- 只扫描新文件及修改过的文件. 只扫描新文件及修改过的文件可极大提升系统相应速度，同时牺牲极少一点安全性。
- 扫描压缩包内容. 包含感染文件的压缩文档不会对您的电脑安全立即造成威胁。只有当恶意程序被从压缩文件中解压出来，而且在实时防护未开启时运行，才会对电脑造成破坏。不过，建议使用此选项以检测并删除任何潜在威胁，即便它并非立即产生威胁。



注意

扫描压缩文件加长扫描时间，并好用更多系统资源。

- 操作选项. 使用此处的选项指定针扫描出的对各类不同文件的处理方式。有三种被检测出的文件:
  - 被感染的文件. 被检测为感染的文件匹配上了 BitDefender 病毒库中的一个特征。BitDefender 通常可以从被感染的文件中删除掉恶意代码，将文件恢复到原始状态。这个操作被称作“清除”。



注意

病毒特征是从真实恶意程序中提取的代码片段，由反病毒程序用来执行模式匹配以检测恶意程序。

BitDefender病毒特征库是由 BitDefender 恶意软徐分析师每小时更新的恶意软件特征集合。

  - 可疑文件. 文件被启发式分析引擎检测为可疑。可以文件无法被清除，因为没有可用清除例程。
  - 隐藏文件(Rootkit). 请注意这些隐藏文件并非您故意在Windows中设置隐藏的，这些文件是由特殊的程序隐藏的，通常称为 rootkit。Rootkit 本质上并非恶意，但是它们常被用来防止反病毒软件检测出病毒或间谍软件。

  除非有很强的理由，否则您不应修改针对检测到的文件的默认操作。

  要设置新的操作，请点击当前的 首选操作 并从菜单中选择所需的操作。指定当首选操作失败时采取的 备选操作。

点击 确定 保存更改并关闭窗口。要运行任务，请点击 扫描。

设置扫描对象

您不能修改 系统扫描任务 分类中扫描任务的扫描对象。您只能查看系统扫描任务的扫描对象。要查看某个系统扫描任务的扫描对象，请右键点击该任务，并选择 显示任务路径。

要为一个用户扫描任务指定扫描目标，请用右键点击该任务，并选择 路径。此外，如果您已经在该任务的属性窗口中，则直接选择 路径 标签页即可。

您可以看到本地磁盘，网络磁盘和可移动磁盘的列表，先前添加的文件或文件夹除外(如果有的话)。当运行这个任务时，所有选中的项目将被扫描。

下列按钮可用：

- 添加项目 - 打开一个窗口浏览并选择您想扫描的文件及文件夹。



注意
您也可以使用拖放功能向列表中添加文件/文件夹。

- 删除条目 - 删除之前加入到列表中的文件及文件夹。

除了这些按钮意外，还有一些选项可帮您快速选择扫描位置。

- 本地磁盘 - 扫描本地磁盘。
- 网络磁盘 - 扫描所有的网络磁盘。
- 可移动驱动器 - 扫描可移动驱动器（光盘、软盘、U盘等)。
- 所有项目 - 扫描所有驱动器，无论是本地、网络或可移动驱动器。

点击 确定 保存更改并关闭窗口。要运行任务，请点击 扫描。

设置扫描任务运行计划

如果遇到复杂的任务，扫描的过程将需要一些时间去完成，您最好关闭所有其他程序。当您不再使用计算机和您的计算机处于空闲状态时去扫描，计划这样的扫描任务是最佳的选择。

要查看或修改某个任务的计划任务设置，请右键点击该任务并选择 计划任务。如果您已经在此任务的属性窗口中，请选择计划任务 标签页。

您可以看到任务计划，如果有的话。

在设置任务的运行计划时，您需要选择下列选项之一：

- 无计划 - 仅在用户请求时运行任务。
- 一次 - 仅在特定时间运行该任务一次。指请在 开始日期/开始时间 设置开始运行的日期和时间。
- 周期运行 - 从指定日期和时间开始，按一定时间间隔（分、小时、日、星期、月等） 周期性运行此扫描任务。
- 于系统启动时 - 在用户登录Windows后的指定时间内启动扫描任务。

点击 确定 保存更改并关闭窗口。要运行任务，请点击 扫描。

15.3. 配置扫描排除

有些时候您可能需要排除某些文件的扫描。 例如，您可能想在实时扫描的时候排除一个eicar测试文件或者请求式扫描时排除 .avi 文件。

BitDefender允许从实时扫描或请求式扫描时排除对象，或从两种扫描中排除。这项功能是为了减少扫描时间，以避免干扰您的工作。

有两种类型的对象可以被排除扫描：

- 路径 – 由一个路径表示的文件或文件夹（包括其中的所有对象）将会被扫描程序排除扫描。
- 文件扩展名 – 所有包含指定文件扩展名的文件将会被跳过扫描，无论其位于硬盘什么位置。

从即时扫描中排除的对象将不会被扫描，不管他们是由您访问还是由一个应用程序访问。



注意

排除项对右键扫描不起作用。右键菜单扫描是一种手动扫描：右键点击想扫描的文件或文件夹并选择 使用BitDefender扫描。

15.3.1. 排除扫描文件或文件夹

要排除扫描路径：

1. 打开 BitDefender。
2. 根据您所使用的用户界面视图模式不同，参照下述说明继续：

   中级视图

       前往 安全 标签并点击窗口左侧 “快速扫描” 区域的 配置反病毒。

       前往 排除 标签。

   专家视图

       前往 反病毒 > 排除。

   注意

   在 “基本视图” 和 “中级视图” ，您可配置快捷方式以便从图表板访问这些设置。更多信息 请参阅 “我的工具” （第 27 页）。

3. 选择对应的复选框以启用扫描排除项。
4. 参照以下说明运行配置向导：
   - 邮件点击 “文件及文件夹” 表格并选择 添加新路径。

- 点击位于排除列表上部的 添加 按钮。

5. 请遵循配置向导执行。您可使用 下一步 和 上一步 按钮在向导中导航。要退出向导，请点击 取消。
   a. 选择“不扫描文件或路径”。此步骤仅在您通过点击 添加 按钮运行向导时出现。
   b. 要指定排除扫描的路径，请使用下述方法之一：
      - 点击 浏览，然后选择要被排除的文件或路径，接着点击 添加。
      - 在编辑栏输入您想要排除扫描的路径，并单击 添加。

      路径将出现在列表中，您可添加任意多的路径。
   c. 默认情况下，选定的路径被排除在实时防护和手动扫描。要更改何时应用排除规则，请点击右边的栏并选择你希望的选项。
   d. 强烈建议您在把路径添加到白名单列表之前对它们进行扫描，以确保它们是干净无毒的。选中复选框以便在添加到白名单之前扫描这些文件。

      点击 完成 添加扫描排除项。
6. 点击 应用 保存修改。

15.3.2. 排除扫描文件扩展名

要排除扫描文件扩展名：

1. 打开 BitDefender。
2. 根据您所使用的用户界面视图模式不同，参照下述说明继续：

   中级视图
      前往 安全 标签并点击窗口左侧“快速扫描”区域的 配置反病毒。

      前往 排除 标签。

   专家视图
      前往 反病毒 > 排除。



注意

在“基本视图”和“中级视图”，您可配置快捷方式以便从图表板访问这些设置。更多信息 请参阅 “我的工具”（第 27 页）。

3. 选择对应的复选框以启用扫描排除项。
4. 参照以下说明运行配置向导：

   - 在扩展名表格中点击右键并选择 添加新扩展名。
   - 点击位于排除列表上部的 添加 按钮。

5. 请遵循配置向导执行。您可使用 下一步 和 上一步 按钮在向导中导航。要退出向导，请点击 取消。
   a. 选择“不扫描文件扩展名”选项。此步骤仅在您通过点击 添加 按钮运行向导时出现。
   b. 要指定排除的文件扩展名，请采用下述方法之一：
      - 从下拉列表中选择您想排除的文件扩展名，并点击 添加。



注意
该菜单包含所有在您系统内注册的所有扩展名列表。当您选择一个文件扩展名，您可以看到它的描述，如果有的话。

      - 在编辑框中输入您想排除的文件扩展名并点击 添加。

      文件扩展名将出现在表中，您可添加任意多的文件扩展名。
   c. 默认情况下，选定的文件扩展名被排除于实时防护和手动扫描，要修改何时应用排除规则，请点击右侧栏并选择所需选项。
   d. 强烈建议强烈建议扫描带有指定文件扩展名的文件，以确保它们未被感染。

      点击 完成 添加扫描排除项。
6. 点击 应用 保存修改。

15.3.3. 管理扫描排除项

如果已添加的扫描排除项不再需要，建议您删除它们或禁用扫描排除。

要管理扫描排除项：

1. 打开 BitDefender，点击位于窗口右上角的 设置 并选择 专家视图。
2. 前往 反病毒 > 排除。

要从列表中删除一个对象，请选择它然后点击 删除 按钮。

要修改一个条目，请选中它并点击 编辑 按钮。一个新的窗口将出现，您可以改变被排除的扩展名或路径和您希望他们在必要时被排除扫描的类型。作必要的修改，然后单击 确定。



注意
您也可以右键点击一个对象，并使用快捷菜单上的选项进行编辑或删除。

要禁用扫描排除项，请清除对应的复选框。

15.4. 隔离区

BitDefender允许将被感染文件或可疑文件到一个名叫“隔离区”的安全区域。文件被放到隔离区后，将不能感染其他文件，同时您可将它们发送给BitDefender实验室做进一步分析。



注意
当一个病毒被隔离后，就不再有任何危害，因为它将不能被执行和打开。

此外，BitDefender 在每次升级病毒库后还会扫描隔离区里的文件。被去除病毒的文件会自动被移动回原来的位置。

要查看并管理隔离区文件，或配置隔离区选项：

1. 打开 BitDefender。
2. 根据您所使用的用户界面视图模式不同，参照下述说明继续：

中级视图
前往 安全 标签并点击窗口左侧“快速扫描”区域的 配置反病毒。

前往 隔离区 标签。

专家视图
前往 反病毒> 隔离区。



注意
在“基本视图”和“中级视图”，您可配置快捷方式以便从图表板访问这些设置。更多信息 请参阅 “我的工具”（第 27 页）。

管理被隔离的文件

点击 发送 可以将隔离区内任何选定的文件发送到BitDefender实验室。默认情况下，BitDefender每隔60分钟提交一次隔离区的文件。

要删除一个被隔离的文件，请选中它并点击 删除 按钮。

如果您想将隔离区中的一个文件恢复到原始位置，请选中它并点击 恢复。

配置隔离区设置

要配置隔离区设置，请点击 设置。使用隔离区设置，您可以设置BitDefender自动执行下列操作：

删除旧文件。. 要自动删除旧的被隔离文件，请选中相应的选项。您必须指定被隔离的文件将保留的天数，以及BitDefender 检查旧文件的频率。

自动提交文件。. 要自动提交被隔离的文件，请选中相应的选项。您必须指定提交文件的频率。

升级后扫描隔离区文件。. 要在每次升级后自动扫描隔离文件，请选中检查相应的选项。如果您想在扫描后自动将安全的文件恢复到原始位置，请选择 恢复安全的文件。

点击 确定 保存修改并关闭窗口。

16. 反网络钓鱼保护

BitDefender反钓鱼功能在您上网时提醒您可能存在钓鱼风险的网页，从而保护您的个人信息不被泄露。

BitDefender为下列软件提供实时反钓鱼防护：

- Internet Explorer
- Mozilla Firefox
- 雅虎通
- Windows Live (MSN) Messenger

16.1. 配置防钓鱼白名单

您可配置并管理一个网站白名单，其中的网站不会被 BitDefender 防钓鱼引擎扫描。白名单应只包含您完全信任的网站。例如，添加您经常上的购物网站。



注意

您可以方便地从集成到浏览器上的BitDefender反钓鱼工具栏添加网站到白名单。更多信息 请参阅 “在 IE 和 Firefox 中管理 BitDefender 钓鱼防护” (第 68 页)。

要配置管理防钓鱼白名单：

- 如果您使用的是支持的浏览器，请点击 BitDefender 工具条 并从菜单中选择白名单。
- 另外，可以遵循下列步骤：
  1. 打开 BitDefender，点击位于窗口右上角的 设置 并选择 专家视图。
  2. 前往 反病毒 > 防护。
  3. 点击 白名单。

要向白名单中添加网站，请在对应的编辑框中输入网址，然后点击 添加。

如果要从白名单中删除一个网站，请点击 移除按钮。

点击 保存 保存所做的修改并关闭窗口。

16.2. 在 IE 和 Firefox 中管理 BitDefender 钓鱼防护

Bitdefender采用直观易用的工具条形式整合到下列的浏览器中：

- Internet Explorer
- Mozilla Firefox

您可以通过集成到上述浏览器中的Bitdefender反钓鱼工具条方便地管理反钓鱼防护和网站白名单。

反钓鱼工具栏图标 在浏览器的上方。点击打开工具条菜单。



注意
如果您没有看到工具条，打开 视图 菜单，指向 工具栏 并选中 BitDefender工具栏。

工具栏包含下面的命令菜单:

- 启用/禁用 – 启用/禁用当前网页浏览器上的 Bitdefender 反钓鱼工具栏。
- 设置 – 打开一个窗口，您可以指定反钓鱼工具栏的设置。您可做以下选择:
  - 实时反钓鱼网页防护 – 实时检测钓鱼网站并警告您。此选项仅控制针对当前网页浏览器的 BitDefender 反钓鱼防护。
  - 添加白名单之前询问 – 当您添加网站到白名单时询问您。
- 添加至白名单 – 添加当前网站到白名单。



重要
添加网站到白名单中后，Bitdefender将不会扫描该网站是否有钓鱼企图。我们建议您只添加您完全信任的网站到白名单中。

- 白名单 – 打开白名单。更多信息 请参阅 "配置防钓鱼白名单" (第 68 页)。
- 报告为钓鱼网站 – 向 BitDefender 实验室报告您认为该网站为钓鱼网站。报告钓鱼网站，可以帮助其他用户免遭信息偷窃。
- 帮助 – 打开帮助文件。
- 关于 – 打开一个包含Bitdefender及支持信息的窗口。

17. 搜索建议

搜索建议在搜索结果页面直接显示搜索结果是否安全，从而帮助您防止钓鱼及不受信任网站对您的侵害。

搜索建议可以在任何浏览器中工作，它检查最流行的搜索引擎的搜索结果：

- Google
- 雅虎
- Bing

搜索建议会在搜索结果前放置一个小图标，告诉您此链接安全与否。

带对号的绿色圆圈： 您可安全访问此链接。
带叹号的红色圆圈： 这是一个钓鱼或不被信任的网页。您应避免打开该链接。
如果您使用 IE 或 Firefox 准备打开一个网页，BitDefender 会自动阻止网页并显示一个警告网页。如果您想忽视警告仍然访问网页，请参照警告网页中的提示进行。

17.1. 禁用搜索建议

要禁用搜索建议：

1. 打开 BitDefender，点击位于窗口右上角的 设置 并选择 偏好设置。
2. 前往 安全设置。
3. 使用开关关闭搜索建议。

18. 隐私控制

BitDefender监控着您系统中可能被间谍软件利用的“热点”，同时检查所有对您的系统和软件的修改。这可有效阻止黑客安装在系统中的木马和其他恶意软件，保护您的私密信息不被窃取（如信用卡号码等）。

隐私控制包括如下组件:

- 隐私控制 – 确保您的个人信息不会泄露。此功能扫描从您电脑发出的电子邮件及聊天消息，以及通过网页发送的数据，并根据您创建的隐私控制规则拦截包含个人信息的通讯。
- 注册表控制 – 当应用程序试图修改注册表项以在系统启动时自动执行时，征询您的许可。
- Cookie控制 – 当新网站试图设置Cookie时，征询您的许可。
- 脚本控制 – 当网站试图运行一个脚本或其他活动内容时征询您的许可。

默认情况下，只有隐私控制被启用。您必须配置合适的身份控制规则，以防止未经授权的机密信息发送。更多信息 请参阅 “配置隐私控制” （第 73 页)。

隐私控制的另一个组件是交互式的。如果启用它，您将看到警告窗口提示，询问您在浏览新网站或安装新软件时是允许还是阻止特定操作。此选项通常建议高级用户使用。

18.1. 设置防护级别

防护级别可帮您方便地启用或禁用隐私控制组件。

要设置防护级别:

1. 打开 BitDefender，点击位于窗口右上角的 设置 并选择 专家视图。
2. 前往 隐私控制 > 状态。
3. 确认隐私控制已启用。
4. 有两个选项:
   - 拖动滑杆设置合适的防护级别。点击 默认级别 将滚动条放到默认级别位置。

     参考滑动条右侧的描述选择适合您安全需求的防护级别。
   - 您也可点击 自定义级别 自己定义防护级别。会出现一个窗口，选择您想要启用的防护控制并单击 确定。

18.2. 身份控制

隐私控制保护您的敏感数据免受在线窃取。

考虑一个简单例子：您创建了一个保护信用卡号码的隐私控制规则。如果间谍软件用某种途径安装到了您的电脑上，它们将无法通过电子邮件、聊天工具或网页发送您的信用卡信息。而且您的孩子们也无法将信用卡信息泄露给网上的其他人。

欲了解更多信息，请参加这些主题：

- "关于隐私控制" （第 72 页）.
- "配置隐私控制" （第 73 页）.
- "管理规则" （第 75 页）.

18.2.1. 关于隐私控制

保证私密数据的安全是一个困扰我们的大问题。数据失窃随着互联网通讯的发展而愈加严重，并利用最新技术欺骗用户交出私密信息。

无论是您的电子邮件或信用卡号码，只要它们落入了恶意之手，就会给您带来损失：您可能会发现自己淹没在垃圾邮件中，或者发现巨额的信用卡消费。

隐私控制保护您的敏感数据免受在线窃取。基于您创建的规则，隐私控制扫描从您计算机发出的网页、电子邮件和即时通讯通信中是否包含特定字符串（例如，您的信用卡号码）。如果发现匹配，则对应的网页、电子邮件或即时讯息会被阻止。

您可创建规则来保护您认为需要保密的任何信息，比如电话号码、身份证号码、银行卡号、电子邮件地址等。本功能支持多用户，使用不同的Windows用户账户登录可以设置不同的个人信息防护规则。如果您的 Windows 帐户是系统管理员帐户，您所创建的规则也可以应用到此计算机上使用其他帐户登录的用户。

为什么要使用个人信息控制?

- 个人信息控制可以非常有效地阻止记录键盘敲击的间谍软件。这种类型的恶意软件记录您的击键顺序并通过互联网将记录发送给黑客。黑客可以从获得的记录中找出敏感信息，例如银行卡号和密码，并从中获利。

  假设这样的应用程序设法避免了被杀毒软件检测到，但是您创建了合适的个人信息保护规则，那么该程序还是无法通过电子邮件、网页或即时通讯将偷窃的数据发送出去。

- 个人信息控制还可以保护您免受 钓鱼 侵害（试图窃取个人信息）。最常见的钓鱼式攻击企图利用欺骗性的电子邮件，引诱你在一个虚假的网页上提交个人信息。

  例如，您可能会收到一封电子邮件，声称是来自您的银行，并请您立即更新您的银行帐户信息。电子邮件中提供了到银行网页的链接，让您去那里提交个人信息。虽然它们看起来是合法的，但是电子邮件中链接指向的网页是虚假的。如果您点击电子邮件中的链接并在虚假网页上提交了您的个人信息，您就会把自己的个人信息发送给了设计这个钓鱼欺骗的黑客。

  但是如果您已经设置了合适的个人信息保护规则，除非您设置了例外，否则您就不能通过网页提交您的个人信息数据。

- 使用隐私控制规则，您可防止孩子们不小心泄露家长的信息（如家庭地址或电话号码）。此外，如果您创建了保护信用卡号码的规则，孩子们就不能未经您同意使用信用卡在网上购物。

18.2.2. 配置隐私控制

如果您想要使用的隐私控制，请执行下列步骤：

1. 打开 BitDefender，点击位于窗口右上角的 设置 并选择 专家视图。
2. 前往 隐私控制 > 个人信息。
3. 确认隐私控制已启用。



注意
如果选项无法被配置，请前往 状态 标签并启用"隐私控制"。

4. 创建规则以保护您的敏感数据。更多信息 请参阅 "创建隐私保护规则"（第 73 页）。
5. 需要时您可以定义特定的排除规则。例如，如果您已创建了保护信用卡号码的规则，则需将您经常输入信用卡号码的网站加入排除列表。更多信息 请参阅 "定义例外规则"（第 74 页）。

创建隐私保护规则

要创建个人信息保护规则，请点击 添加 按钮，并按照配置向导的引导进行操作。您可使用 下一步 和 上一步 按钮在向导中导航。要退出向导，请点击 取消。

1. 欢迎窗口
2. 设置规则类型和规则数据

   您必须设置下列参数：

   - 规则名称 – 请在此输入规则的名称。
   - 规则类型 – 选择规则类型（地址、姓名、信用卡、身份证等）。
   - 规则数据 – 请输入您希望保护的数据。例如，如果您要保护您的信用卡号码，在这里输入全部或部分号码。

   重要
   如果您输入少于三个字符，系统会提示您验证数据。我们推荐您至少输入三个字符，以避免造成误堵的讯息及网页。

   所有您输入的数据都会被加密，为了加强安全性，请不要输入您要保护的信息的全部数据。

3. 选择通讯类型及用户

a. 选择您希望BitDefender扫描的通信类型。

- 扫描网页(HTTP流量) - 扫描HTTP (网页)流量并阻止匹配上规则的外传数据。
- 扫描电子邮件(SMTP流量) - 扫描SMTP (电子邮件) 流量并阻止包含规则数据的外发电子邮件。
- 扫描即时通讯流量 - 扫描即时通讯流量并阻止包含规则数据的外发聊天信息。

您可以仅当规则全部匹配字符串或大小写匹配字符串时应用此规则。

b. 指定该规则适用的用户。

- 仅我自己(当前用户) - 规则将只应用于您的用户帐户。
- 受限用户帐户 - 规则将应用于您和所有受限 Windows 帐户。
- 所有用户 - 规则将被应用于所有 Windows 帐户。

4. 规则说明

在编辑框中输入对此规则的简短说明。由于当您查看规则时，需要被被阻止的数据（字符串）不是明文显示的，规则说明能帮助您了解该规则的用途。

点击完成。规则将会显示在表格中。

从现在起，任何企图通过电子邮件、聊天工具及网页发送指定数据的操作都会失败。您会看到一个警告，通知您 BitDefender 已经拦截了涉及隐私的数据被发送。

定义例外规则

在有些情况下，您需要为特定的识别规则定义例外。当您创建规则时，防止您的信用卡号码不被发送的HTTP(网页)。每当您的信用卡号码，从您的用户账号中提交到一个网站时，相关的网页会被阻止。例如，您想在一个在线商店购买鞋类(您知道是安全的)，您需要在相关的规则下指定一个例外。

要打开管理例外规则的窗口，请点击 例外规则。

要添加例外，按照下列步骤进行:

1. 点击 添加 按钮添加一个新的条目。
2. 双击 指定排除的项目 并输入您想添加为例外规则的网址、电子邮件地址或即时通讯联络人。
3. 双击 流量类型，并从菜单中选择和您之前输入的地址类型对应的选项。
   - 如果您指定的是一个网站地址，请选择HTTP。
   - 如果您已经指定了一个电子邮件地址，请选择 电子邮件(SMTP)。
   - 如果您指定了即时通讯联系人，请选择 即时通讯。

要从列表中删除一个例外规则，请选中它并点击 删除 按钮。

点击 确定 保存修改。

18.2.3. 管理规则

要管理隐私控制规则：

1. 打开 BitDefender，点击位于窗口右上角的 设置 并选择 专家视图。
2. 前往 隐私控制 > 个人信息。

您可以在表格中看到已创建的规则列表。

要删除一个规则，选中它并点击 删除 按钮。

要编辑一条规则，请选中它并点击 编辑 按钮，或者直接双击它。一个新窗口会显示出来。在这里，您可以更改规则名称，描述和参数(类型,数据和通讯)。 单击 确定 以保存更改。

18.3. 注册表控制

Windows操作系统有个非常重要的组件叫 注册表，Windows在此记录其设置选项、已安装的程序、用户信息及其他很多信息。

注册表 还被用作定义哪些程序在Windows启动时会自动启动，病毒经常利用这一点以便在用户重启电脑时自动加载。

注册表控制 对Windows注册表保持关注 - 对于检测木马是十分有效的。 程序需要在Windows启动时自动运行而修改注册表项时，会及时提醒您。更多信息 请参阅 “注册表警报” (第 31 页)。

要配置注册表控制：

1. 打开 BitDefender，点击位于窗口右上角的 设置 并选择 专家视图。
2. 前往 隐私控制 > 注册表。
3. 选择对应的复选框以启用注册表控制。



注意
如果选项无法被配置，请前往 状态 标签并启用“隐私控制”。

管理规则

要删除一个规则，选中它并点击 删除 按钮。

18.4. Cookie 控制

Cookie 在互联网中非常常见。它们是存储在您计算机上的小文件，您访问的网站在您的计算机上创建Cookie文件以记录您的特定信息。

Cookie 的主要目的是让您访问网站更方便，例如，网站可以借助Cookie记住您的姓名和偏好，这样您不必在每次访问该网站时都输入这些信息。

但是Cookie同样可以被用作跟踪您的上网习惯，从而触及您的隐私。

这是 Cookie 控制帮助。Cookie 控制启用后会在您访问需要设置 Cookie 的新网站时询问您是否允许。更多信息 请参阅 “Cookie 警报” （第 32 页）。

配置 Cookie 控制:

1. 打开 BitDefender，点击位于窗口右上角的 设置 并选择 专家视图。
2. 前往 隐私控制 > Cookie。
3. 选择对应的复选框启用 Cookie 控制。



注意
如果选项无法被配置，请前往 状态 标签并启用“隐私控制”。

4. 您可为经常访问的网站设置规则，但是必要性不大。根据您的回答，在警告窗口中会自动创建规则。



注意
由于互联网上巨量的Cookie被使用，Cookies控制 开始使用时可能相当烦人，因为开始时它会询问很多有关某网站要在您的计算机上设置Cookie的问题。不过当您把您常用的网站都添加到规则表中后，上网就会变得和以前一样方便。

手动创建规则

要手动创建规则，请点击 添加 按钮并在设置窗口中配置规则参数。您可以设定下述参数:

- 域名 – 输入要应用规则的域名。
- 操作 – 选择规则的操作。

操作	描述
允许	允许该域名上的Cookie操作。
拒绝	不允许域名上的Cookie操作。

- 方向 – 选择通信的方向。

类型	描述
发送	规则只对发向网站的Cookie生效。
接收	规则只对接收自网站的Cookie生效。
两者	规则对发送和接收的Cookie都生效。



注意
您可以接受cookies，但不返回他们，通过设置操作 拒绝 和方向 传出。

点击完成。

管理规则

要删除一个规则，选中它并点击 删除 按钮。要修改规则参数，请选择该规则并点击 编辑 按钮，或者双击它，然后在配置窗口中进行所需修改。

18.5. 脚本控制

脚本 及 ActiveX控件和Java applets 等代码被用于创建交互式网页，它们可被编写为具有危害行为。例如，ActiveX控件可以获取对您计算机数据的完全控制，可以读取您的数据、删除信息、截获密码并截取您上网时的邮件。您应当只接受来自您信赖网站的脚本。

如果启用脚本控制，您在访问运行脚本或其他活动内容的新网站时，会被询问是否允许。更多信息 请参阅 “脚本警报” （第 32 页)。

要配置脚本控制：

1. 打开 BitDefender，点击位于窗口右上角的 设置 并选择 专家视图。
2. 前往 隐私控制 > 脚本。
3. 选择对应的复选框以启用脚本控制。



注意
如果选项无法被配置，请前往 状态 标签并启用“隐私控制”。

4. 您可为经常访问的网站设置规则，但是必要性不大。根据您的回答，在警告窗口中会自动创建规则。

手动创建规则

要手动创建规则，请点击 添加 按钮并在设置窗口中配置规则参数。您可以设定下述参数：

- 域名 – 输入要应用规则的域名。
- 操作 – 选择规则的操作。

操作	描述
允许	该域名上的脚本将被执行。
拒绝	该域名上的脚本将不会执行。

点击完成。

管理规则

要删除一个规则，选中它并点击 删除 按钮。要修改规则参数，请选择该规则并点击 编辑 按钮，或者双击它，然后在配置窗口中进行所需修改。

19. 漏洞检测

要保证计算机不受黑客和恶意程序的侵害，一个非常重要的防范措施是保持您的操作系统和常用软件是最新版本。此外，为防止对您计算机的非授权访问，必须为每个WIndows用户账户设置强密码（不能被轻易破解的密码）。

BitDefender定期检查您的系统漏洞，并通知您存在的问题。

19.1. 检查是否有漏洞

您可使用 漏洞检测 向导一步步检查漏洞并进行修复。要运行向导，请打开 BitDefender 并根据用户视图的不同选择如下操作:

中级视图
: 前往 安全 标签页并点击窗口左侧“快速任务”区域的 漏洞扫描。

专家视图
: 前往 漏洞 > 状态 并点击 立即检查。

遵循六步向导移除电脑中的漏洞。您可使用 下一步 按钮在向导中导航，要退出向导，请点击 取消。

1. 保护您的计算机

   选择要检查的漏洞。

2. 扫描所选项目...

   请等待 BitDefender 完成系统漏洞检测。

3. Windows 更新

   您可看到您的计算机上尚未安装的Windows关键及非关键更新列表。选择要安装的更新。

4. 应用程序更新

   如果应用程序不是最新版本，请点击后面的链接下载最新版本。

5. 弱密码

   您可以看到您计算机上的Windows用户账户列表，以及每个账户的密码强度。点击 修复 修改弱密码。

6. 摘要

   您可在此查看操作结果。

19.2. 状态

要查看当前漏洞状态，启用/禁用自动漏洞扫描，请参照以下步骤:

1. 打开 BitDefender，点击位于窗口右上角的 设置 并选择 专家视图。

2. 前往 漏洞 > 状态。

表中显示在上次漏洞检测中发现的问题及其状态。如果有解决方案的话，您也能在表中看到。如果操作是 无，则该问题不是一个漏洞。



重要

要想收到系统及程序漏洞的自动通知，请保持 自动漏洞扫描开启。

根据问题的不同，修复一个特定漏洞的步骤如下：

- 如果 Windows 更新可用，请点击 安装（位于 操作 列)以进行安装。
- 如果某程序不是最新，请点击 更多信息 查看版本信息，并从产品网站找到最新版本的下载链接。
- 如果某个 Windows 账户密码强度不高，请点击 查看 & 修复 以强制用户在下次登录时修改密码，或者由您为其修改密码。强密码是指组合了大写和小写字母、数字及特殊字符（#、$ 和 @）的密码。
- 如果 Windows “媒体自动运行”功能被启用，请点击 修复 将其禁用。

19.3. 设定

要配置自动漏洞检测，请遵循下述步骤：

1. 打开 BitDefender，点击位于窗口右上角的 设置 并选择 专家视图。
2. 前往 漏洞 > 设置。
3. 选择您想定期检查的系统漏洞前面的复选框。
   - Windows 关键更新
   - Windows 常规更新
   - 应用程序更新
   - 弱密码
   - 媒体自动运行



注意

如果您清除了某类漏洞前的复选框，BitDefender将不会通知您相关问题。

20. 聊天加密

您的网络聊天消息将只会在您和您的聊天对象之间传送。加密聊天后，聊天内容将不会被其他人窃听。

默认情况下，如果满足下列条件，Bitdefender会加密您所有的聊天内容：

- 您的聊天对象装有支持即时通讯加密的Bitdefender产品，并且启用了针对该即时通讯软件的加密功能。
- 您和您的聊天伙伴使用雅虎通或MSN。



重要
如果您的聊天对象使用了网页聊天工具（如网页版雅虎通和MSN），或者其他支持雅虎通和MSN的软件，Bitdefender将不会加密聊天内容。

要配置聊天消息加密：

1. 打开 BitDefender，点击位于窗口右上角的 设置 并选择 专家视图。
2. 前往 加密 > 聊天加密。



注意
您可以通过 聊天窗口上的 BitDefender 工具条 轻松设置聊天加密功能。

默认情况下，启用针对雅虎通和MSN的即时通讯加密。您可选择禁用针对某个聊天工具的加密或完全禁止此功能。

会显示两个列表：

- 加密例外 – 列出禁用即时通讯加密的聊天联系人及对应聊天工具。要从列表中删除一个联系人，请选中他然后点击 移除 按钮。
- 当前连接 – 列出当前的即时通讯连接（用户名和聊天程序），以及是否启用加密。以下原因会导致某些连接不被加密：
  - 您明确禁用对该联系人加密。
  - 您的联系人没有安装支持即时通讯加密的BitDefender版本。

20.1. 禁用对特定用户的加密

要禁用对特定用户的加密，请执行下列步骤：

1. 点击 打开 按钮打开配置窗口。
2. 在编辑框中输入联系人的用户账号。
3. 选择与该用户关联的即时通讯软件。
4. 点击 确定。

20.2. 位于聊天窗口的 BitDefender 工具条

您可以通过聊天窗口上的Bitdefender工具栏轻松设置即时通讯加密功能。

工具条在聊天窗口的右下角，带有 BitDefender LOGO。



注意

工具条通过在 BitDefender LOGO旁边显示一个小钥匙 ，来表明对话被加密。

点击 BitDefender 工具条可以设置如下选项：

- 永久禁用针对 联系人 的加密。.
- 邀请 联系人 使用加密. 要加密会话，您的联系人必须安装 BitDefender，并使用兼容的即时通讯程序。

21. 游戏/笔记本模式

游戏/笔记本模式模块可让您设置BitDefender的特殊运行模式:

- 游戏模式　暂时修改产品设置以便在您玩游戏时将产品对系统资源的消耗降到最低。
- 笔记本模式 在笔记本电脑使用电池时不运行计划任务,以延长电池使用时间。
- 静默模式 暂时修改产品设置从而在您观看电影或做演示的对您打扰最小。

21.1. 游戏模式

游戏模式暂时修改防护设置,以使产品对系统性能的影响最低。在游戏模式下,会应用以下设置:

- 所有Bitdefender警报和弹出窗口都被禁用。
- Bitdefender实时防护级别设置为 宽松。
- 不进行升级。



注意

要更改此设置,请前往 升级>设置 并清除 在游戏模式下不进行升级 复选框。

默认情况下,当您运行一个BitDefender已知的游戏,或者某个应用程序全屏幕运行时,BitDefender会自动进入游戏模式。您也可以使用默认热键 Ctrl+Alt+Shift+G 进入游戏模式。强烈建议您在结束游戏后退出游戏模式(您可以使用相同的默认热键 Ctrl+Alt+Shift+G)。



注意

在游戏模式下,您可以看到字母 G 叠加在 BitDefender 系统托盘图标上。

要配置游戏模式:

1. 打开 BitDefender,点击位于窗口右上角的 设置 并选择 专家视图。
2. 前往 游戏/笔记本模式 > 游戏模式。

在窗口的上方,您可看到游戏模式的状态。您可点击 游戏模式已启用 或 游戏模式已关闭 修改当前状态。

21.1.1. 设置自动游戏模式

自动游戏模式允许BitDefender在检测到运行游戏时自动进入游戏模式。您可以配置下列选项:

- 使用BitDefender内置的游戏列表 – 当您运行BitDefender列表中的已知游戏时自动进入游戏模式。要查看此列表，请点击 管理游戏，然后点击 游戏列表。
- 全屏操作 – 您可选择当程序全屏运行时自动进入游戏模式或静默模式。
- 询问我是否将全屏程序加入游戏列表 – 在离开全屏模式时，询问您是否将新应用程序加入游戏列表。通过添加新的应用程序到游戏列表，下次启动它时BitDefender将自动进入游戏模式。



注意
如果您不希望 BitDefender 自动进入游戏模式，请清除 启用自动游戏模式 复选框。

21.1.2. 管理游戏列表

BitDefender在您运行游戏列表中的程序时会自动进入游戏模式。要查看和管理游戏列表，请点击 管理游戏。接着会显示一个新窗口。

以下情况下，新的应用程序会自动添加到列表中：

- 您启动了一个BitDefender已知游戏列表中的游戏。要查看列表，请点击 游戏列表。
- 在离开全屏模式时，您从提示窗口将应用程序添加到了游戏列表。

如果您想对某个应用程序禁用自动游戏模式，请清除对应的复选框。您应该对运行全屏模式的常用应用程序禁用自动游戏模式，比如浏览器和视频播放器。

要管理游戏列表，您可以使用表格上方的按钮：

- 添加 – 添加新的应用程序到游戏列表。
- 删除 – 从游戏列表中删除一个应用程序。
- 编辑 – 编辑游戏列表中的条目。

21.1.3. 添加或修改游戏

当您向游戏列表中添加条目或编辑已有条目时，一个新窗口会出现：

点击 浏览 选择应用程序或输入该程序的全路径。

如果您不希望所选的程序启动时自动进入游戏模式，请选择 禁用。

点击 确认 将该条目加入游戏列表。

21.1.4. 配置游戏模式设置

要设置计划任务的特性，请使用下述选项：

- 允许此模块修改病毒扫描计划任务 – 防止病毒扫描计划任务在游戏模式时运行。您可以选择下列选项之一：

选项	描述
跳过任务	不要运行计划任务。
推迟执行任务	退出游戏模式后立即执行计划任务。

21.1.5. 修改游戏模式热键

您可手动进入游戏模式，使用默认Ctrl+Alt+Shift+G热键。如果您想改变热键，请按照下列步骤：

1. 点击 高级设置。接着会显示一个新窗口。
2. 在使用热键选项下面，设置您希望使用的热键：
   - 通过选中下面的功能键来设置热键：Ctrl键Ctrl，Shift键Shift，Alt键Alt。
   - 在编辑框中输入您使用的普通键。

   例如，如果您想使用 Ctrl+Alt+D热键，您需要选中 Ctrl 和 Alt 并输入 D。



注意
清除 使用热键 旁的复选框将禁用热键。

3. 点击 确定 保存修改。

21.2. 笔记本模式

笔记本模式是专为笔记本用户设计的，其目的是当笔记本靠电池供电时，使BitDefender对电池消耗降到最低。

在笔记本模式下，默认不运行计划任务。

BitDefender检测到您的笔记本切换到电池供电时会自动进入笔记本模式。同样，BitDefender检测到您的笔记本不再用电池供电时会自动退出笔记本模式。

要配置笔记本模式：

1. 打开 BitDefender，点击位于窗口右上角的 设置 并选择 专家视图。
2. 前往 游戏/笔记本模式 > 笔记本模式。

您可看到笔记本模式是否启用。如果笔记本模式已启用，BitDefender将在笔记本用电池供电时应用配置的选项。

21.2.1. 设置笔记本模式选项

要设置计划任务的特性，请使用下述选项：

- 允许此模块修改病毒扫描计划任务 – 防止病毒扫描计划任务在笔记本模式时运行。您可以选择下列选项之一：

选项	描述
跳过任务	不要运行计划任务。
推迟执行任务	退出笔记本模式时立即运行计划任务。

21.3. 静默模式

静默模式暂时修改防护设置，以使产品对系统性能的影响最低。在静默模式下以下选项会被使用：

- 所有Bitdefender警报和弹出窗口都被禁用。
- 默认禁用任务计划。

默认情况下，BitDefender 在您播放电影或演示，以及程序进入全屏状态时，会自动进入静默模式。强烈建议您在看完电影或演示后退出静默模式。



注意
在静默模式下，您会发现系统图盘区的 BitDefender 图标略有变化。

要配置静默模式：

1. 打开 BitDefender，点击位于窗口右上角的 设置 并选择 专家视图。
2. 前往 游戏/笔记本模式 > 静默模式。

在窗口上方，您可看到静默模式状态。您可点击 静默模式已启用 或 静默模式已禁用 以修改当前状态。

21.3.1. 配置全屏操作

您可以配置下列选项：

- 全屏操作 – 您可选择当程序全屏运行时自动进入游戏模式或静默模式。



注意
如果您不想让 BitDefender 自动进入静默模式，请清除 全屏操作 复选框。

21.3.2. 配置静默模式选项

要设置计划任务的特性，请使用下述选项：

- 允许此模块修改病毒扫描计划任务 – 防止病毒扫描计划任务在静默模式时运行。您可以选择下列选项之一：

选项	描述
跳过任务	不要运行计划任务。
推迟执行任务	在退出静默模式后立即运行计划中的任务。

22. 家庭网络

家庭网络模块可让您从一台计算机上管理你家里所有计算机上的Bitdefender产品。要访问家庭网络模块，请打开 BitDefender 并根据用户视图的不同选择如下操作:

中级视图
　　前往 网络 标签。

专家视图
　　前往 家庭网络管理。



注意
您可添加一个到 我的工具 的快捷方式。

要管理安装在您家里各台计算机上的Bitdefender产品，请按照下列步骤进行:

1. 在您的电脑上开启 BitDefender 家庭网络管理。将您的电脑设置为“服务器”。
2. 将每台您希望管理的计算机加入家庭网络（设定密码）。将每台电脑都设置为“普通”。
3. 回到您的计算机，并将所有你希望管理的计算机加入家庭网络。

22.1. 启用 BitDefender 家庭网络

要启用 BitDefender 家庭网络管理，请遵循下述步骤:

1. 点击 启用家庭网络。系统会提示您设置家庭网络管理密码。
2. 请在两个编辑框输入相同的密码。
3. 在 BitDefender 家庭网络管理中设置电脑的角色:
   - 服务器 – 对管理其他电脑的电脑设置此选项。
   - 普通电脑 – 对于将被服务器电脑管理的电脑，请选择此选项。
4. 点击 确定。

您将看到计算机名出现在家庭网络地图中。

禁用网络按钮会显示。

22.2. 向家庭网络中添加计算机

任何符合下述标准的电脑都会被自动添加到家庭网络:

- BitDefender 家庭网络已对其启用。
- 角色被设置为“普通电脑”。
- 在启用网络时设置的网络与在服务器电脑上设置的密码相同。



注意
在“专家视图”中，您可随时点击 自动发现 按钮扫描家庭网络中符合条件的电脑。

要从服务器电脑手动添加电脑到 BitDefender 家庭网络，请参照下述步骤：

1. Click 添加电脑.
2. 请输入家庭网络管理密码并点击 确定。接着会显示一个新窗口。

   您可看到家庭网络中所有计算机的列表。图标含义如下：

   表示一台在线但是没有安装Bitdefender产品的电脑。
   表示一台在线并且安装了Bitdefender产品的电脑。
   表示一台离线的安装了Bitdefender产品的电脑。
3. 请执行如下操作之一：
   - 从列表中选择计算机名称加入。
   - 在对应区域输入要加入的计算机的IP地址或计算机名称。
4. 点击 添加。系统会提示您输入该计算机的家庭网络管理密码。
5. 输入在该计算机上设置的家庭网络管理密码。
6. 点击 确定。如果您提供了正确的密码，选定计算机的名称会出现在家庭网络图中。

22.3. 管理家庭网络

成功创建了Bitdefender家庭网络之后，您可以从一台计算机上管理所有计算机上的BitDefender产品。

移动鼠标光标到网络图中的一台计算机上，您可以看到该计算机的简要信息（名称、IP地址、影响系统安全的问题数、注册状态等）。

点击网络地图中的一个电脑名，您会看到您在远程电脑上可以执行的所有管理任务。

- 为此计算机注册BitDefender

  通过输入授权密钥注册此电脑上的 BitDefender。
- 为远程计算机设置配置密码

  创建密码，限制对此电脑上的 BitDefender 设置的访问。
- 运行手动扫描任务

  允许您在远程电脑上运行手动查杀。您可执行下述扫描任务之一：我的文档扫描、系统扫描或深度系统扫描。
- 修复此计算机中的所有问题

  允许您遵循 修复全部问题 向导修复影响电脑安全的问题。

- 查看历史/事件

  允许您访问安装在此电脑上的 BitDefender 的 历史记录 模块。

- 立即更新

  为安装在此电脑上的 BitDefender 启动升级过程。

- 设为此网络中的更新服务器

  允许您设置此电脑为家庭网络升级服务器，所有其他家庭网络中的电脑可从此电脑进行更新。使用此选项将降低互联网流量，因为网络中只有一台电脑会连接到互联网下载更新。

- 移除家庭网络中的计算机

  将电脑从家庭网络中移除。

当 BitDefender 界面处于中级视图时，您可通过点击相应按钮同时在所有受管理的电脑上运行任务。

- 扫描全部 – 同时扫描所有您管理的计算机。
- 升级全部 – 升级您所管理的所有计算上的BitDefender产品。
- 注册全部 – 同时注册您管理的所有计算机上的BitDefender产品。

在某台计算上运行任务之前，系统会提示您输入家庭网络管理密码。请输入家庭网络管理密码并点击 确定。



注意

如果您计划执行多项任务，您可选择本次操作期间不要再次显示此消息。选择此选项，您在本次操作期间将将不会再次被提示输入密码。

23. 更新

每天都会发现新病毒，所以需要及时更新BitDefender病毒库。

如果您是通过宽带或DSL连接到互联网，BitDefender会自行处理升级事宜。默认情况下，产品在您启动计算机时检查更新，随后每 小时 进行一次检查。

如果发现了新升级包，可能会要求您确认进行升级，也可能自动进行升级，这取决于自动升级设置 里面的设置选项。

升级过程是逐步执行的，需要被更新的文件会被逐步替换，因此升级过程不会影响产品的正常运行，同时又可减少系统漏洞。



重要

要能不受最新病毒的侵害，请保持启用 自动升级。

升级主要有以下几种类型:

- 反病毒引擎升级 – 随着新威胁的出现，病毒库也需要得到升级以防护最新病毒。这种升级类型也称作 病毒定义升级。
- 反间谍软件引擎升级 – 新的间谍软件特征将被添加到数据库中，这种升级类型也称作 反间谍软件升级。
- 产品升级 – 当产品新版本发布时，会增加新功能和扫描技术以提升产品的性能。这种升级类型也称作 产品升级。

23.1. 运行更新

任何时候您只需点击 立即升级 就可完成自动升级。这种升级方式也称作 用户请求的升级。

要更新 BitDefender，根据用户界面视图的不同，遵循不同的步骤:

基本视图
: 点击位于“保护您的电脑”区域的 立即更新 图标。

中级视图
: 前往 安全 标签并点击窗口左侧“快速任务”区域的 立即更新。

专家视图
: 前往 更新 > 更新。

升级 模块会连接到BitDefender Update Server并检查是否有可用更新，如果发现了可用更新，则会根据在 手动升级设置 里的选择，提示您确认升级或者直接自动进行升级。



重要

升级完成后，可能有必要重新启动计算机。建议立刻重新启动。



注意

如果您通过拨号方式连接到网络，建议您定期手动升级产品。更多信息 请参阅 “如果在网速较慢的电脑上更新 BitDefender” （第 106 页）。

23.2. 配置更新设置

升级可通过本地网络、互联网进行，可直接连接或通过代理服务器连接。默认情况下， BitDefender每小时通过互联网检查更新，并在不通知您的情况下安装新的升级包。

要配置更新设置:

1. 打开 BitDefender，点击位于窗口右上角的 设置 并选择 专家视图。
2. 前往 更新 > 设置。
3. 按照需要配置选项。想了解某个选项的具体含义，将鼠标放在该选项上面，在窗口底部就会显示描述。
4. 点击 应用 保存修改。

要应用默认设置，请选中 默认.。

升级设置选项分为四个功能组（升级服务器设置，自动升级设置，手动升级设置 和 高级设置）。 以下将分别说明每个功能组。

23.2.1. 设置更新服务器

要设置升级服务器，请使用 升级服务器设置 部分的选项。



注意

只有当您连接到一个存储BitDefender病毒库在本地网络，或者当您使用代理服务器连接到互联网，才配置这些设置。

要拥有更快速可靠的升级，您可以指定两个升级服务器：一个 首选升级服务器 和 一个 备选升级服务器。 默认情况下，两个升级服务器是相同的： http://upgrade.bitdefender.com。

要修改其中一个更新位置，提供本地镜像网址在URL编辑区，在您想改变的相关位置。



注意

建议您将首选升级服务器设置为本地服务器，而不更改备选升级服务器，作为在本地服务器出现故障时的容灾方案。

如果您的公司使用代理服务器连接到互联网，请选中 使用代理，然后点击 代理服务器设置 配置代理服务器选项。欲了解更多信息，请参加“连接设置” （第 45 页）

23.2.2. 设置自动升级

要向让 BitDefender 自动进行升级，请设置 自动升级设置 中的选项。

您可在 升级间隔 编辑栏指定两次连续升级检测的时间间隔。默认情况下，更新时间间隔为1小时。

要指定自动升级过程如何进行，请选择下述选项之一：

- 静默升级 - BitDefender 将自动下载和安装更新。
- 下载升级包之前提示 - 每次发现可用升级包时，会提示您下载。
- 安装升级包之前提示 - 每次下载一个升级包之后，系统会在安装前提示您。

23.2.3. 手动升级设置

指定手动升级（用户请求的升级）如何执行，您可在 手动升级设置 组中指定一个选项：

- 静默升级 - 手动升级将自动在后台进行，无需用户干预。
- 下载升级包之前提示 - 每次发现可用升级包时，会提示您下载。

23.2.4. 设置高级设置选项

为防止 BitDefender 升级过程打扰您的工作，您可在 高级设置 组中设置相关的选项：

- 等待重启而不提示 - 如果升级后需要重启，产品会继续用旧文件运行，直到系统重启。用户不会被提示进行重启，用户的工作不会被打扰。
- 在进行扫描时禁止升级 - 在扫描进行时BitDefender将不会进行升级，这样 BitDefender 升级进程不会干扰扫描任务。



注意

如果BitDefender在扫描进行时被升级，扫描过程将被中止。

- 当游戏模式启用时不进行跟新 - BitDefender 在游戏模式启用时将不会进行更新。这样，可以在游戏模式时将产品对系统性能的影响降到最低。
- 启用更新共享 - 如果您想最小化更新时网络流量对系统性能的影响，请使用更新共享选项。
- 从此电脑上传 BitDefender 文件 - BitDefender 允许您和其他 BitDefender 用户分享最新的病毒库数据。

如何…

24. 如何扫描文件及文件夹?

使用 BitDefender 进行扫描非常简单灵活。有多种方式设置 BitDefender 扫描文件及文件夹中的病毒。

- 使用 Windows 右键菜单
- 使用扫描任务
- 使用扫描工具条

当您启动一个扫描后，防病毒扫描向导会出现，并引导您完成扫描过程。欲了解关于向导的更多信息，请参阅 “反病毒扫描向导” （第 55 页）。



注意

要了解如何在 Windows 安全模式下使用 BitDefender 扫描，请参考 “如何在安全模式下扫描我的电脑? ” （第 112 页）。

24.1. 使用 Windows 右键菜单

这是扫描您计算机中文件或文件夹的最简单方式，也是推荐的方式。右键点击您想扫描的对象并从菜单中选择 使用BitDefender扫描。按照反病毒扫描向导的指引完成扫描。

使用这种扫描方式的典型应用场景包括:

- 您怀疑一个特定的文件或文件夹被感染。
- 从互联网下载的文件，您认为比较危险。
- 在复制文件到您的计算机前，扫描网络共享。

24.2. 使用扫描任务

如果您想定期扫描计算机或指定的文件夹，您可以考虑使用扫描任务。扫描任务告诉 BitDefender 扫描的路径、扫描的选项及采取的操作。此外，您还可以 设定计划任务 指定任务在特定的时间定期运行。

要用扫描任务扫描您的计算机，您需要打开 BitDefender 界面并运行所需的扫描任务。根据您所在的用户界面视图不同，运行扫描任务所需执行的步骤稍有不同。

在基本视图运行扫描任务

在基本视图，您只能运行几个预先配置的扫描任务。点击 安全 按钮并选择所需的扫描任务。按照反病毒扫描向导的指引完成扫描。

在中级视图中运行扫描任务

在中级视图中，您可以运行多个预置的扫描任务。您还可配置自定义的扫描任务，以使用自己设置的扫描选项扫描电脑上指定的位置。参照以下步骤在中级视图中运行扫描任务。

1. 点击 安全 标签。
2. 在左侧的“快速任务”区域，点击 全面系统扫描 并选择所需的扫描任务。要配置运行一个自定义扫描，请点击 自定义扫描。
3. 按照反病毒扫描向导的指引完成扫描。如果您选择运行一个自定义扫描，您必须完成自定义扫描向导。

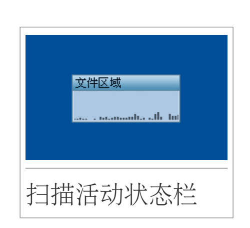
在专家视图中运行扫描任务

在专家视图中，您可以运行所有预先配置的扫描任务，还可以修改它们的扫描选项。此外，如果你想扫描计算机中的特定位置，您还可以创建自定义的扫描任务。遵循以下步骤在专家视图中运行扫描任务。

1. 点击左侧菜单的 反病毒。
2. 点击 病毒扫描 选项卡。您可在此发现数个默认的扫描任务，并可创建您自己的扫描任务。
3. 双击您想运行的扫描任务。
4. 按照反病毒扫描向导的指引完成扫描。

24.3. 使用扫描工具条

扫描活动条 以图形化方式显示您系统上的扫描活动。这个小窗口默认只在 专家视图 中可用。



扫描活动状态栏

您可以用扫描活动条快速扫描文件或文件夹。将您想扫描的文件或文件夹拖放到扫描活动条上。按照反病毒扫描向导的指引完成扫描。



注意
更多信息 请参阅 “扫描活动状态栏” （第 18 页）。

25. 如何创建自定义扫描任务?

要创建扫描任务，请打开 BitDefender 并根据用户视图的不同选择如下操作:

中级视图

前往 安全 标签并点击窗口左侧“快速任务”区域的 自定义扫描。

您会看到一个向导，帮您穿件扫描任务。您可使用 下一步 和 上一步 按钮在向导中导航。要退出向导，请点击 取消。

1. 欢迎
2. 选择目标

   点击 添加对象 选择您想扫描的文件及文件夹。

   点击 高级设置。在 概览 标签中，将鼠标移动到滑动条上调整扫描选项。如想详细配置扫描选项，请点击 自定义。前往 计划任务 标签选择人物开始时间。
3. 完成

   您可在此输入任务名称，并将扫描任务添加到“快速任务”区域（可选）。

   点击 开始扫描 创建任务并运行扫描向导。

专家视图

1. 前往 反病毒 > 病毒扫描。
2. 点击 新任务，您会看到一个新窗口。



注意

您也可右键点击预定义的扫描任务，如 深度系统扫描 然后选择 复制任务。这在建立新任务时非常有用，因为您可通过修改复制的扫描任务快速创建一个新任务。

3. 在 概览 标签页输入任务名称并移动活动条调整扫描选项。

   如想详细配置扫描选项，请点击 自定义。
4. 前往 路径 标签选择扫描对象。点击 添加项目 选择要扫描的文件或文件夹。
5. 前往 计划任务 标签选择人物开始时间。
6. 点击 确定 保存任务。新的复制任务将出现在用户自定义任务中，它可以在这个窗口中编辑、删除或运行。

26. 如何设置定时扫描?

定期扫描计算机是确保计算机远离病毒的良好实践。使用 BitDefender 可以设置扫描任务从而自动扫描您的计算机。

请按照如下步骤设置 BitDefender 计划任务扫描您的计算机:

1. 打开 BitDefender。
2. 根据您所使用的用户界面视图模式不同,参照下述说明继续:

   中级视图
   : 前往 安全 标签并点击窗口左侧 “快速扫描” 区域的 配置反病毒。

   专家视图
   : 点击左侧菜单的 反病毒。

3. 点击 病毒扫描 选项卡。您可在此发现数个默认的扫描任务,并可创建您自己的扫描任务。

   - 系统任务可运行于每个 Windows 账户。
   - 用户任务只能由创建它们的用户运行。

   以下是您可创建计划任务的默认扫描任务:

   全面系统扫描
   : 扫描整个计算机,不扫描压缩文档。默认配置下,该任务扫描除 rootkits 之外的所有类型恶意软件。

   快速扫描
   : 快速扫描使用了云技术检测运行在您电脑中的恶意程序。快速扫描通常少于一分钟,占用的系统资源是普通病毒扫描的很小一部分。

   自动登录扫描
   : 扫描当用户登录到Windows操作系统时被运行的项目。要使用此任务,您需要设定其在系统启动时运行。默认情况下,自动登录扫描被禁用。

   深度系统扫描
   : 扫描整个系统,包括压缩文档。在默认配置下,它扫描威胁到您系统安全的所有类型的恶意软件,如病毒,间谍软件,广告软件, rootkit和其他。

   我的文档
   : 使用这项任务扫描当前用户的重要文件夹:我的文档,桌面 和 启动 。这会确保您的文档和工作环境安全,并保证系统启动时运行的应用程序是安全的。

   如果这些扫描任务都不能满足您的需求,您可以创建一个新的扫描任务,并设置其任务计划。

4. 右键点击要设置的扫描任务然后选择 计划任务。接着会显示一个新窗口。

5. 按照需求设置运行计划任务：
   - 要想只运行一次扫描任务，选择 一次 并指定开始日期和时间。
   - 要想在系统启动之后运行扫描任务，请选择 于系统启动时。您可以指定在系统启动后多长时间运行此扫描任务。
   - 要向定期运行扫描任务，请选择 周期性 并指定频度和开始日期、时间。



注意

丽日，如果想在每周六凌晨两点扫描您的计算机，您可以按照下面的示例配置计划任务：

a. 选择 周期性。

b. 在 每隔 部分，输入 1 并从菜单中选择 周。这样，计划任务会每周运行一次。

c. 将开始日期设置为下个星期六。

d. 将开始时间设置为 2:00:00 AM。

6. 点击 确定 保存计划任务。该扫描任务将会按照您设置的计划自动运行。如果在计划任务预定运行时间计算机关机，则该任务将在您下次打开计算机时运行。

27. 如何使用代理服务器更新 BitDefender?

通常 BitDefender 会自动检测并导入您电脑的代理服务器设置。如果您通过代理服务器连接到互联网，您需要了解代理服务器设置信息并配置BitDefender 的相应选项。欲知如何操作，请参见 "如何找到我的代理服务器设置?"（第 123 页）。

找到代理服务器设置后，请遵循以下步骤:

1. 打开 BitDefender，点击位于窗口右上角的 设置 并选择 专家视图。
2. 前往 常规 > 设置。
3. 点击 代理服务器设置，位于 连接设置。
4. 在对应输入框输入代理服务器设置。
5. 点击 确定。



注意

如果此信息未能帮您解决问题请联系我们的客服中心，参见 "客服"（第 116 页）。

28. 如何升级到其他 BitDefender 2011 产品?

使用 BitDefender 2011 您可轻松从一个 BitDefender 2011 产品升级到另一个产品。

请设想如下情况：您已使用 BitDefender Antivirus Pro 2011 2011 一段时间，最近想转换到 BitDefender 全功能安全套装 2011 以获得更多功能。

您所需做的就是购买一个适用于您想升级到的 BitDefender 2011 产品的授权密钥，并将其输入您当前使用的 BitDefender 2011 中。

按照下述步骤执行：

1. 打开 BitDefender。
2. 点击窗口底部的 授权密钥信息 链接。您会看到注册窗口。
3. 输入授权密钥并点击 立即注册。
4. BitDefender 会通知您授权密钥适合另一个不同产品，并允许您安装它。点击相应的链接并遵循包含三个步骤的指导说明执行升级。
   a. 确认操作
   b. 正在更新

      请等待 BitDefender 完成升级过程。需要花费几分钟时间。
   c. 更新已完成

      已完成处理，您可能需要重启电脑。

寻求援助和获得帮助

29. 疑难解答

本章说明您在使用 BitDefender 中可能遇到的问题，并提供可能的解决方案。绝大部分此类问题都可通过正确配置产品设置选项解决。

如果您在这里没有找到自己遇到的问题，或者此处给出的解决方案无法解决您的问题，您可以联系 BitDefender 的用户服务人员，参见 “客服” （第 116 页）。

29.1. 安装问题

本文帮您解决在安装 BitDefender 时的常见问题。问题可被划分为以下几类：

- 安装验证错误：因为您的电脑系统状况，安装向导无法运行。
- 安装失败：您运行了安装向导，但是没有成功完成。

29.1.1. 安装验证错误

当您运行安装向导时，向导会验证您电脑的多个条件，以确保能够安装产品。下表列出常见的安装验证错误及解决方法。

错误	描述&解决方案
您没有足够的权限安装此软件。	要运行安装向导安装 BitDefender 您需要有管理员权限。请执行下列操作之一： ● 用 Windows 管理员帐户登录并运行安装程序。 ● 邮件点击安装文件并选择 以管理员身份运行。输入一个 Windows 管理员帐户的用户名和密码。
安装程序检测到之前安装的 BitDefender 版本没有被正确卸载。	您的电脑此前安装过 BitDefender，但是没有被彻底卸载，这会阻止安装新的 BitDefender 产品。 要解决此问题，请参照如下步骤操作： 1. 前往 www.bitdefender.com/uninstall 下载卸载工具。 2. 用管理员权限运行卸载程序。 3. 重启您的电脑。 4. 运行安装向导并安装 BitDefender。
BitDefender 和您的操作系统不兼容。	您正在一个 BitDefender 不支持的操作系统上进行安装。请检查 “系统需求” （第 2 页） 了解 BitDefender 支持的操作系统。

错误	描述&解决方案
	如果您的操作系统是 Windows XP SP1 或未安装服务包的 Windows XP，您需要安装微软的 XP SP2 或更高版本服务包，然后再次运行安装程序。
安装文件适用于各种类型的处理器。	如果您看到这个错误，说明您运行了安装文件的错误版本。BitDefender 安装文件有两个版本，一个适用于32位处理器，一个适用于64位处理器。 要确保您拥有正确的版本，请从 www.bitdefender.com 直接下载安装文件。

29.1.2. 安装失败

安装失败有多个可能原因：

- 在安装过程中显示错误窗口。您可能会被提示取消安装，或者点击一个按钮运行卸载工具清理您的电脑。



注意
在您开始安装后，您可能会被提示磁盘空间不足以安装 BitDefender。 这种情况下，请在您准备安装 BitDefender 的磁盘上清理出足够的空间，然后再继续安装。

- 安装程序卡住，您的系统也可能停止响应。只有重启系统才能恢复系统正常。
- 安装已经完成，但是您无法使用 BitDefender 的部分或全部功能。

要查找安装失败原因并重新安装，请参照下面的步骤：

1. 在安装失败后清理系统。. 如果安装失败，BitDefender 的注册表项和文件可能会有部分残留在您的电脑中。这些残留可能会阻止新的安装，还可能影响系统性能和稳定性。因此在安装前请先清理这些残留。

   在此情况下，最简易的解决方案是彻底卸载 BitDefender 并重装。更多信息 请参阅 "如何彻底卸载 BitDefender？" （第 124 页）。
2. 验证安装失败的可能原因。. 在您继续重装之前，请验证并修复可能导致安装失败的原因：

   a. 请检查您是否安装了其他安全软件，它们会干扰 BitDefender 的正常运行。如果是这种情况，建议您卸载所有其他安全软件并重装 BitDefender。

   b. 您还应该检查电脑是否染毒。请执行下列操作之一：

      - 使用 BitDefender 急救光盘扫描您的电脑并清除存在的病毒。更多信息 请参阅 "BitDefender救援光盘" （第 109 页）。
      - 打开IE，访问 www.bitdefender.com 并运行在线扫描（点击 the scan online 按钮）。

3. 尝试重装 BitDefender。建议您从官方网站 www.bitdefender.com 下载并运行最新的安装包。
4. 如果安装仍然失败，请联系我们的客服中心，参见 “客服” （第 116 页）。

29.2. 我的电脑有点卡

通常在安装安全软件之后，电脑会稍微变慢，这一般是正常的。

如果您发现明显变慢，可能是因为如下原因：

- BitDefender 不是电脑上安装的唯一安全软件。

  虽然 BitDefender 会在安装时查找并删除其他安全软件，但是建议您最好在安装 BitDefender 之前先卸载其他安全软件。更多信息 请参阅 “如何卸载其他安全软件？” （第 122 页）。

- 运行 BitDefender 的最低系统要求未达到。

  如果您的电脑未符合最低系统要求，电脑将会变得很卡，尤其是在同时运行多个程序时。更多信息 请参阅 “最低系统需求” （第 2 页）。

- 您的硬盘碎片极多。

  文件碎片会减缓文件访问速度，降低系统性能。

  要使用 Windows 操作系统清理磁盘碎片，请按照以下顺序点击： 开始 → 所有程序 → 附件 → 系统工具 → 磁盘碎片整理。

29.3. 扫描未开始

出现这种类型的问题可能有两个原因：

- 之前安装的 BitDefender 未完全卸载，或错误的 BitDefender 安装。

  在此情况下，最简易的解决方案是彻底卸载 BitDefender 并重装。更多信息 请参阅 “如何彻底卸载 BitDefender？” （第 124 页）。

- BitDefender 不是电脑上安装的唯一安全软件。

  在此情况下，遵循如下步骤：

  1. 卸载其他安全软件。更多信息 请参阅 “如何卸载其他安全软件？” （第 122 页）。
  2. 从电脑中彻底删除 BitDefender。
  3. 重装 BitDefender。

如果此信息未能帮您解决问题请联系我们的客服中心，参见 “客服” （第 116 页）。

29.4. 我无法再使用一个程序

当您准备运行一个在安装 BitDefender 之前正常的程序时，会出现此问题。

您可能遇到下述情况:

- 您会从 BitDefender 收到一条消息,提示您程序正准备对系统做修改。
- 您可能会从您尝试使用的程序收到一条错误消息。

此类情况发生时因为活动病毒控制模块错误地将某些程序检测为病毒。

活动病毒控制是 BitDefender 中监控运行的程序并报告其潜在风险行为的功能模块。由于此功能基于启发式技术,可能会出现正常程序被活动病毒控制报告的情况。

当此情况发生时,您可将相应程序从活动病毒控制的监控中排除。

要将程序加入到排除列表,请遵循下述步骤:

1. 打开 BitDefender,点击位于窗口右上角的 设置 并选择 专家视图。
2. 前往 反病毒 > 防护。
3. 点击 高级设置。
4. 前往新窗口中的 排除 标签,点击 添加 按钮并浏览到程序 .exe 文件所在目录(通常在 C:\Program Files)。
5. 点击 确定 保存修改并关闭窗口。
6. 关闭 BitDefender 窗口并检查问题是否仍然存在。

如果此信息未能帮您解决问题请联系我们的客服中心,参见 "客服" (第 116 页)。

29.5. 如果在网速较慢的电脑上更新 BitDefender

如果您的网络连接较慢(如拨号上网),更新过程可能出现错误。

要保证电脑包含最新 BitDefender 病毒库,请遵循以下步骤:

1. 打开 BitDefender,点击位于窗口右上角的 设置 并选择 专家视图。
2. 前往 更新 > 设置。
3. 在 手动扫描设置 中,选择 下载更新前提示。
4. 点击 应用 并前往 更新 标签页。
5. 点击 立即更新,您将会看到一个新窗口。
6. 仅选择 病毒库更新 然后点击 确定。
7. BitDefender 将只下载并安装病毒库更新。

29.6. 我的电脑没有连到互联网,该如何更新 BitDefender?

如果您的电脑没有联网,您必须手动在一台联网的电脑上下载更新,然后拷贝到您的电脑上。

按照下述步骤执行:

1. 在可以上网的电脑上，打开浏览器并前往网址：

   www.bitdefender.com/site/view/Desktop-Products-Updates.html

2. 在 手动更新 列，点击对应您产品及系统架构的链接。如果您不清楚您的 Windows 是 32 位还是 64 位，请参见 “使用 32 位还是 64 位 Windows？”（第 123 页）。
3. 保存文件 weekly.exe 到电脑。
4. 将下载的文件拷贝到移动存储设备如 U 盘上，然后再拷贝到您的电脑。
5. 双击文件并遵循向导指示操作。

29.7. BitDefender 服务无响应

本文帮您解决 BitDefender 服务无响应 错误。您可能遇到此错误的场景：

- 位于 系统托盘 的 BitDefender 图标变灰，并弹出通知提示 BitDefender 服务无响应。
- BitDefender 主界面显示 BitDefender 服务无响应。

这个错误可能由下面的情况之一引发：

- 正在安装一个重要更新。
- BitDefender 服务之间的通讯临时出现错误。
- 部分 BitDefender 服务被停止。
- 在您的电脑上同时运行着其他的安全软件。
- 您电脑上的病毒影响 BitDefender 的正常运行。

要解决此问题，请尝试下述方法：

1. 稍等几分钟看看状态是否有变化。错误可能只是暂时的。
2. 重启计算机并等待一会儿，直到 BitDefender 启动。打开 BitDefender 主界面看看问题是否还存在。重启电脑通常就能解决此问题。
3. 请检查您是否安装了其他安全软件，它们会干扰 BitDefender 的正常运行。如果是这种情况，建议您卸载所有其他安全软件并重装 BitDefender。
4. 如果错误持续存在，可能是因为更严重的问题（例如，您的电脑感染了病毒，病毒干扰了 BitDefender 的运行）。请联系客户服务中心，参见 “客服”（第 116 页）。

29.8. BitDefender 卸载失败

本文帮助您解决在卸载 BitDefender 时可能遇到的问题。有两种可能：

- 卸载中出现错误提示窗口。窗口中会显示一个运行卸载工具的按钮，运行该工具可彻底卸载 BitDefender。

- 卸载程序卡住，系统也停止响应。点击 取消 终止卸载，如果还未解决问题，请重启系统。

如果卸载失败，BitDefender 的注册表项和文件可能会有部分残留在您的电脑中。这些残留可能会阻止新的安装，还可能影响系统性能和稳定性。要想彻底卸载BitDefender，请运行卸载工具。

更多信息 请参阅 “如何彻底卸载 BitDefender？”（第 124 页）。

如果此信息未能帮您解决问题请联系我们的客服中心，参见 “客服”（第 116 页）。

30. 从您的电脑中删除恶意程序

恶意程序可用很多种方法危害您的电脑，BitDefender 采取的操作根据恶意程序的不同而不同。由于病毒频繁修改其行为，建立其行为及操作的模式非常困难。

有时 BitDefender 无法自动删除电脑中的恶意程序。在此情况下，需要您的干预。

如果您在这里没有找到自己遇到的问题，或者此处给出的解决方案无法解决您的问题，您可以联系 BitDefender 的用户服务人员，参见 “客服” （第 116 页）。

30.1. BitDefender救援光盘

BitDefender 救援光盘 是包含在 BitDefender 安装光盘中的一个功能，允许您在操作系统开始前扫描并清除所有硬盘。还可帮助您从已经中毒的电脑中将数据保存到移动存储设备。

如果您没有 BitDefender 救援光盘，可从这个网址下载其 ISO 映像文件：

http://download.bitdefender.com/rescue_cd/

下载 .iso 文件并使用刻录软件将其刻录到光盘上。

使用 BitDefender 救援光盘扫描电脑

要使用 BitDefender 救援光盘扫描系统，请遵循以下步骤：

1. 设置您电脑的 BIOS 以从光盘启动。
2. 将光盘放入光驱并重启电脑。
3. 请等待 BitDefender 窗口出现并选择 运行BitDefender 救援光盘。
4. 等待启动完成，这会持续一会儿。
5. 启动完成后，BitDefender 病毒库会自动更新，并会对所有检测到的硬盘进行一次扫描。

使用 BitDefender 救援光盘保存数据

假设您因为某些原因不能启动您的Windows计算机，同时您需要访问计算机上的一些重要数据，此时可以使用 BitDefender 救援光盘来帮您。

要想将数据从电脑复制到移动设备，如 U盘，请参照以下步骤：

1. 设置您电脑的 BIOS 以从光盘启动。
2. 将光盘放入光驱并重启电脑。
3. 请等待 BitDefender 窗口出现并选择 运行BitDefender 救援光盘。
4. 等待启动完成，这会持续一会儿。

5. 启动完成后，BitDefender 病毒库会自动更新，并会对所有检测到的硬盘进行一次扫描。

   您的硬盘分区将出现在桌面。要以类似 Windows 资源管理器的方式查看其内容，请双击它。



注意
使用 BitDefender 救援光盘时，您将会处理 Linux 类型的磁盘分区名。在 Windows 下的磁盘将会显示为 [LocalDisk-0] 对应于 Windows 下的 (C:)， [LocalDisk-1] 对应于 (D:)，以此类推。

6. 将移动设备插到电脑的 USB 接口。稍等一会儿您会看到一个显示设备内容的窗口。
7. 您可像在 Windows 中惯用的那样复制文件及文件夹。

如果此信息未能帮您解决问题请联系我们的客服中心，参见 “客服” (第 116 页)。

30.2. 当 BitDefender 在您电脑上发现病毒时怎么办?

您可能通过下述方式了解电脑中存在病毒:

- 您扫描了电脑，并且 BitDefender 发现了感染项目。
- 病毒警告提示您 BitDefender 拦截了一个或多个病毒。

在此情况下，更新 BitDefender 以保证您有最新病毒库，并运行深度系统扫描以分析系统。

在深度扫描完成后，为每个感染项目选择所需操作（清除、删除或移动到隔离区）。



警告
如果您怀疑文件是操作系统文件或并未被感染，请勿遵从这些步骤，并立即联系 BitDefender 客户服务人员。

如果所选操作无法执行，而扫描日志显示一个无法删除的感染文件，您必须手动删除文件。

在正常模式下可用的第一个方法:

1. 关闭 BitDefender 实时病毒防护。欲知如何操作，请参见 “如何启用/禁用实时防护？” (第 124 页)。
2. 显示 Windows 中的隐藏对象。欲知如何操作，请参见 “如何显示 Windows 中的隐藏对象？” (第 124 页)。
3. 找到感染文件（在扫描日志中查看路径）并删除。
4. 启用 BitDefender 实时病毒防护。

当首选操作未能清除感染，请参照下述步骤:

1. 重启您的电脑并进入安全模式。欲知如何操作，请参见 “如何进入安全模式？”（第 122 页）。
2. 显示 Windows 中的隐藏对象。
3. 找到感染文件（在扫描日志中查看路径）并删除。
4. 重启您的电脑并进入正常模式。

如果此信息未能帮您解决问题请联系我们的客服中心，参见 “客服”（第 116 页）。

30.3. 我如何清理的压缩文档的病毒？

压缩文档是指一个包含了以特定压缩格式压缩的诸多文件的文件，从而可以减少磁盘空间占用。

这些格式中有的是开放格式，因此 BitDefender 可以扫描其内部并采取合适的操作去除感染。

其他压缩文档格式部分或全部关闭，BitDefender 只能检测它们内部的病毒，但是无法采取任何操作。

如果 BitDefender 通知您在压缩文件中发现病毒且无可用操作，说明由于压缩文件的权限设置导致无法清除病毒。

您可按如下方法清除压缩文件中的病毒：

1. 运行深度系统扫描找到包含病毒的压缩文件。
2. 关闭 BitDefender 实时病毒防护。
3. 找到压缩文件，用压缩工具解压，比如 WinZip。
4. 找到被感染文件并删除。
5. 删除原始压缩文件以确保病毒被彻底移除。
6. 使用压缩软件重新压缩文件，比如 WinZip。
7. 开启BitDefender 实时防护并运行深度系统扫描以确保系统中没有其他感染文件。



注意
请注意存放在压缩文档中的病毒不会直接对电脑造成威胁，因为病毒需要被解压并执行才能感染您的电脑。

如果此信息未能帮您解决问题请联系我们的客服中心，参见 “客服”（第 116 页）。

30.4. 如何清除邮件附件中的病毒？

BitDefender 还可发现存在于电子邮件数据库及电子邮件附件中的病毒。

有时需要使用扫描日志中的信息找到被感染邮件，并手动删除。

您可按如下方法清除邮件附件中的病毒：

1. 使用 BitDefender 扫描电子邮件数据库。
2. 关闭 BitDefender 实时病毒防护。
3. 打开扫描日志，使用被感染邮件的相关信息（如标题、发件人、收件人）在邮件客户端中找到邮件。
4. 删除被感染邮件。大部分邮件软件会把被删除的邮件移动到一个恢复文件夹，邮件可从该文件夹被恢复。您需要确认邮件同时也从恢复文件夹中被删除。
5. 压缩存储感染消息的文件夹。
   - 在 Outlook Express中：在“文件”菜单中，点击“文件夹”，然后点击“压缩所有文件夹”。
   - Microsoft Outlook：在“文件”菜单，点击“数据文件管理”。选择您希望压缩的个人文件夹(.pst)文件，并点击“设置”。点击“紧凑”。
6. 启用 BitDefender 实时病毒防护。

如果此信息未能帮您解决问题请联系我们的客服中心，参见 “客服” （第 116 页）。

30.5. 如何在安全模式下扫描我的电脑?

BitDefender 手动扫描让您可以扫描指定的文件夹或磁盘分区，而不需要创建一个扫描任务。

此功能可以在 Windows 安全模式下使用。

如果您的系统感染了顽固病毒，无法在正常模式清除，您可以尝试进入 Windows 安全模式，然后用 BitDefender 手动扫描功能扫描每个磁盘分区。

欲了解如何进入安全模式，请参见 “如何进入安全模式? ” （第 122 页）。

1. 要使用 BitDefender 手动扫描，请遵循以下步骤点击：开始 → 所有程序 → BitDefender 2011 → BitDefender 手动扫描。
2. 点击 添加目录 选择扫描对象，您会看到一个新窗口。
3. 选择扫描对象：
   - 要扫描桌面，请选择 桌面。
   - 要扫描整个磁盘分区，请从 我的电脑 中选择。
   - 要扫描指定目录，请浏览并选择对应的目录。
4. 点击 确认 及 继续 开始扫描。
5. 按照反病毒扫描向导的指引完成扫描。

30.6. 当 BitDefender 将正常文件检测为感染文件时怎么办?

有时 BitDefender 会错误地将正常文件报告为威胁（误报）。要纠正此错误，添加文件到 BitDefender 排除区域：

1. 关闭 BitDefender 实时病毒防护。欲知如何操作，请参见 “如何启用/禁用实时防护？”（第 124 页）。
2. 显示 Windows 中的隐藏对象。欲知如何操作，请参见 “如何显示 Windows 中的隐藏对象？”（第 124 页）。
3. 从隔离区恢复文件。
4. 将文件插入排除区域。
5. 启用 BitDefender 实时病毒防护。

如果此信息未能帮您解决问题请联系我们的客服中心，参见 “客服”（第 116 页）。

30.7. 如何从系统卷信息中清除感染文件

系统卷信息文件夹是由操作系统在您的硬盘上创建的一个区域，Windows 在其中存储关键的系统配置信息。

BitDefender 引擎可以检测任何存储于系统卷信息的感染文件，但是由于该位置为保护区域，可能无法清除感染文件。

在系统还原文件夹中发现的感染文件将显示在扫描日志中，例如：

?:\System Volume Information_restore{B36120B2-BA0A-4E5D-…

要立即彻底清除被感染的文件，请禁用然后重新启用系统还原功能。

当系统还原被关闭时，所有的还原点都会被删除。

在系统还原被再次开启时，会根据计划任务及事件需求创建新的还原点。

请遵循以下步骤禁用系统还原：

- Windows XP:
    1. 按以下顺序： 开始 → 程序 → 附件 → 系统工具 → 系统还原
    2. 点击窗口左侧的 系统还原设置。
    3. 选择所有驱动器的 关闭系统还原 复选框，然后点击 应用。
    4. 当您被警示所有存在的还原点都将被删除时，请点击 是 继续。
    5. 要开启系统还原，请不选中所有磁盘上的 关闭系统还原 检查框，并点击 应用。
- Windows Vista:
    1. 请按照如下路径点击：开始 → 控制面板 → 系统维护 → 系统
    2. 点击左侧的 系统防护。

       如果您被提示输入管理员密码或确认，请输入密码或进行确认。
    3. 要关闭系统还原，请清除每个驱动器对应的复选框并点击 确定。

4. 要开启系统还原，请选择对应的磁盘前的复选框并点击 确定。

- Windows 7:

1. 点击 开始，右键点击 电脑 然后点击 属性。
2. 点击位于左侧区域的 系统保护 链接。
3. 在 系统防护 选项，选择每个磁盘盘符并点击 配置。
4. 选择 关闭系统保护 并点击 应用。
5. 当看到提示时，点击 删除，然后点击 继续，最后点击 确定。

如果此信息未能帮您解决问题请联系我们的客服中心，参见 “客服” （第 116 页）。

30.8. 扫描日志中的“密码保护文件”指的是什么？

此消息说明 BitDefender 检测到这些文件被密码保护，或被用其他方式加密。

通常，以下项目为密码保护文件：

- 属于另一个安全软件的文件。
- 属于操作系统的文件。

要实际扫描内容，这些文件需要被解压或解密。

那些文件被解压缩后，BitDefender 的实时防护扫描程序会自动扫描它们并保护您的电脑。如果您想使用 BitDefender 扫描这些文件，您需要联系产品开发公司以告知您文件的详细信息。

建议您忽视这些文件，因为它们不会造成安全问题。

30.9. 扫描日志中的“跳过的项目”指什么？

所有在扫描日志里显示为“跳过”的文件都是安全的。

为提高性能，BitDefender 不扫描自上次扫描后未变化的文件。

30.10. 扫描日志中的“过度压缩”文件指的是什么？

过度压缩项目是指扫描引擎无法解压缩的文件，或者解压时间会过长以致或让电脑不稳定的文件。

过度压缩指 BitDefender 跳过扫描压缩文件内部内容，因为解压该文件耗用系统资源过多。内容将根据需要被实时防护模块检查。

30.11. BitDefender 为何会自动删除感染文件？

如果检测到感染文件，BitDefender 将会自动尝试清除感染。如果清除病毒失败，文件会被移动到隔离区以隔离病毒。

对于特殊类型的恶意软件，由于整个程序都是恶意代码，因此无法做清除处理。此时，恶意文件会被从磁盘上删除。

通常当您从不可信网站下载安装包时会出现此情况。如果遇到此类情况，请从软件出品公司网站或其他可信的下载网站下载安装包。

31. 客服

BitDefender 致力于为我们的用户提供无与伦比的快速精准支持。如果您在使用 BitDefender 产品时遇到问题，您可通过我们丰富的在线资源迅速找到问题解决方案。如果愿意，您也可联系 BitDefender 客服人员。我们的客服人员会及时回答您的问题，并提供您所需的帮助。

31.1. 在线资源

有多个在线资源可帮您解决 BitDefender 相关问题。

- BitDefender 知识库：http://www.bitdefender.com/help
- BitDefender 支持论坛：http://forum.bitdefender.com
- “恶意软件城市”电脑安全门户：http://www.malwarecity.com
- 视频教程

您也可使用搜索引擎了解电脑安全、BitDefender 产品及公司信息。

31.1.1. BitDefender知识库

BitDefender 知识库是BitDefender产品有关信息的在线仓库。您也可以在此轻易地找寻您提出的问题的解决方案。报告是由BitDefender 的支持及开发组提供。它们也同时提供了一些有关反病毒防范措施的文章，BitDefender 管理组的方案和解说以及更多的有趣的文章。

BitDefender知识库是公开的，客户可以通过它进一步地了解病毒，增进对电脑病毒的知识。客户所发来的有效病毒报告以及咨询都即将列入BitDefender 知识库中。

您可以随时在此网址阅读BitDefender档案资料 http://kb.bitdefender.com。

31.1.2. BitDefender 支持论坛

BitDefender 支持论坛为 BitDefender 用户提供了一个方便的方式来获取帮助及帮助他人。

如果您的 BitDefender 产品工作不正常，比如不能从电脑中删除某个病毒，或您对其工作是否正常有疑问，请在技术支持论坛发帖寻求帮助。

BitDefender 技术支持人员发现新帖时会帮助您，您也可能从有经验的 BitDefender 用户那里获得帮助。

在发表新的问题前，请先搜索论坛看看相似主题的帖子。

BitDefender 支持论坛位于 http://forum.bitdefender.com，提供五种语言版本：英语、德语、法语、西班牙语及罗马尼亚语。点击 家庭 & 家庭办公防护 链接以访问适合个人用户的产品。

31.1.3. 恶意软件城市门户

恶意程序城市门户包含丰富的电脑安全信息，您可在此了解当电脑联网时可能遇到的各种安全威胁。帮您了解电脑安全术语的词典。

我们会及时更新最新文章，以向您提供最新的病毒播报、安全趋势及其他和电脑安全相关的信息。

恶意软件城市的网页是 http://www.malwarecity.com。

31.1.4. 视频教程

视频教程会一步步讲解如何配置产品。它们被创建为非常直观的方式，易于理解。

最重要的目标是通过提供基本及中级安全指导原则确保愉快的体验，包括如何使用 BitDefender。

使用视频教程了解如何使用及配置 BitDefender 的详细信息。

例如，不是打电话给 BitDefender 客户支持人员寻求帮助，您也可观看下面视频教程中的说明。

31.2. 请求帮助

问题诊断及帮助 列出您使用此产品时最常遇到的问题。

如果没有找到您遇到的问题的解决方案，您可直接联系我们：

- “从 BitDefender 产品直接联系我们” （第 117 页）
- “通过在线知识库联系我们” （第 118 页）



重要

要联系 BitDefender 客户服务人员，您需要激活 BitDefender 产品。更多信息 请参阅 “注册及我的账号” （第 40 页）。

从 BitDefender 产品直接联系我们

如果能上网，您可从 BitDefender 界面直接联系我们的客户服务寻求支持。

要寻求帮助，您可使用产品内置的支持工具。

依照以下步骤使用内置的支持工具：

1. 打开 BitDefender。
2. 点击位于窗口右下角的 帮助及支持 链接。
3. 您有两个选择：
   - 在我们的数据库中搜索您寻找的信息。
   - 根据您遇到的问题选择其类别。

客户服务 涉及购买、授权、退款及续费。

技术支持 包括产品本身问题和它的功能。

抗击恶意软件 说明和病毒相关的问题。

4. 阅读相关文章并尝试建议的解决方案。
5. 如果该解决方案未解决问题，请使用文中的链接运行支持工具。
6. 输入您的电子邮件地址，选择类别并写下对问题的简短描述。

   点击 下一步。
7. 请稍等，BitDefender 正在收集产品相关信息，此信息将帮助我们的工程师寻找您问题的解决方案。

   点击 下一步。
8. 点击 完成 将信息发送给 BitDefender 客户支持部门，我们会尽快和您联系。

通过在线知识库联系我们

如过无法访问如何使用 BitDefender 产品的信息，请访问我们的在线知识库：

1. 访问 http://www.bitdefender.com/help。BitDefender 知识库包含大量描述和 BitDefender 相关问题解决方案的文章。
2. 请搜索 BitDefender 知识库，寻找可能解决您问题的文章。
3. 阅读相关文章并尝试建议的解决方案。
4. 如果该解决方案未能解决您的问题，请使用文章中的链接联系 BitDefender 客户服务代表。
5. 通过电子邮件、聊天工具或电话联系 BitDefender 客户服务代表。

32. 联系信息

我们相信高效的沟通是业务成功的关键，十年以来，BitDefender 已经建立起了一套超出用户期望的沟通体系。如果您有任何问题，请随时联系我们。

32.1. 网址

销售部：sales@bitdefender.com
技术支持：www.bitdefender.com/help
文档：documentation@bitdefender.com
合作伙伴项目：partners@bitdefender.com
市场部：marketing@bitdefender.com
媒体关系：pr@bitdefender.com
工作机会：jobs@bitdefender.com
提交病毒：virus_submission@bitdefender.com
垃圾邮件提交：spam_submission@bitdefender.com
报告不当使用：abuse@bitdefender.com
产品网址:http://www.bitdefender.com
产品 FTP 存档：ftp://ftp.bitdefender.com/pub
当地分销商：http://www.bitdefender.com/site/Partnership/list/
BitDefender 知识库：http://kb.bitdefender.com

32.2. 当地分销商

BitDefender 本地经销商可帮您了解更多信息。

要查找您所在国家的 BitDefender 分销商：

1. 访问 http://www.bitdefender.com/site/Partnership/list/。
2. BitDefender 当地分销商的联系信息会被自动显示，如果您未看到此信息，请使用左侧菜单中的“分销商查找工具”并选择您所在的国家或地区。
3. 如果在您的国家没有 BitDefender 分销商，请通过电子邮件联系我们 sales@bitdefender.com。请用英语撰写电子邮件，以便我们尽快帮您解决问题。

32.3. BitDefender 各国办事处

BitDefender的分公司都非常乐意在它们的业务区回答您的任何咨询，以下是它们的地址以及电话号码。

美国

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309

电话（办事处&销售): 1-954-776-6262
销售: sales@bitdefender.com
技术支持: http://www.bitdefender.com/help
网址: http://www.bitdefender.com

英国和爱尔兰

Business Centre 10 Queen Street
Newcastle, Staffordshire
ST5 1ED
邮箱: info@bitdefender.co.uk
电话: +44 (0) 8451-305096
销售: sales@bitdefender.co.uk
技术支持: http://www.bitdefender.com/help
网址: http://www.bitdefender.co.uk

德国

BitDefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
办公室: +49 2301 91 84 222
销售: vertrieb@bitdefender.de
技术支持: http://kb.bitdefender.de
网址: http://www.bitdefender.de

西班牙

BitDefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
传真: +34 93 217 91 28
电话: +34 902 19 07 65
销售: comercial@bitdefender.es
技术支持: www.bitdefender.es/ayuda
网站: http://www.bitdefender.es

罗马尼亚

BITDEFENDER SRL
West Gate Park, Building H2, 24 Preciziei Street
Bucharest
传真: +40 21 2641799

销售电话: +40 21 2063470
销售电子邮件: sales@bitdefender.ro
技术支持: http://www.bitdefender.ro/suport
网站: http://www.bitdefender.ro

33. 有用信息

本章介绍一些您在诊断技术问题之前需要了解的重要流程。

在 BitDefender 中定位技术问题需要一些 Windows 知识，因此下一步通常和 Windows 操作系统有关。

33.1. 如何卸载其他安全软件?

使用安全产品的主要原因是保护您的数据安全。当您电脑上安装多个安全软件时会出现什么情况?

在一台电脑上安装多款安全软件，系统会不稳定。BitDefender Antivirus Pro 2011 安装程序自动检测其他安全软件并提供卸载选项。

如果您未在开始安装时卸载其他安全软件，请遵循以下步骤:

- Windows XP:
  1. 点击 开始，前往控制面板 并双击 添加/删除程序。
  2. 正在刷新已安装软件列表，请稍候。
  3. 找到要删除的程序名称并选择 卸载。
  4. 请等待卸载结束，然后重启您的电脑。
- Windows Vista 和 Windows 7:
  1. 点击 开始，然后 控制面板 并双击 程序和功能。
  2. 请稍等片刻，正在准备已安装软件列表。
  3. 找到要删除的程序名称并选择 卸载。
  4. 请等待卸载结束，然后重启您的电脑。

如果您未从电脑中删除其他安全软件，请从该产品网站下载其卸载工具，或了解卸载方法。

33.2. 如何进入安全模式?

安全模式是一种诊断操作模式，主要用户诊断影响 Windows 正常操作的问题。这些问题包括驱动冲突、病毒阻止 Windows 正常启动等。在安全模式下，只有少数程序运行，Windows 只会加载最基本的驱动程序以及最少的操作系统组件。这就是大部分病毒在 Windows 安全模式下会不活跃，并能被移除的原因。

要进入 Windows 安全模式:

1. 重新启动计算机。
2. 在 Windows 启动前点击 F8 几次以调出启动菜单。
3. 在启动菜单中选择 安全模式 并按 Enter。

4. 请等待 Windows 进入安全模式。
5. 此过程结束于一个确认消息。点击 确定 确认。
6. 要正常启动 Windows，请重启电脑即可。

33.3. 使用 32 位还是 64 位 Windows?

要了解您使用的是 32 位还是 64 位操作系统，请参照以下步骤：

- Windows XP:
  1. 点击 开始。
  2. 找到 我的电脑 于 开始 菜单。
  3. 右键点击 我的电脑 并选择 属性。
  4. 如果您看到 x64 版本 列在 系统 下，说明您正在运行 64 位的 Windows XP。
     如果您未看到 x64 版本列出，说明您运行着 32 位 Windows XP。
- Windows Vista 和 Windows 7:
  1. 点击 开始。
  2. 找到 计算机 于 开始 菜单。
  3. 右键点击 计算机 并选择 属性。
  4. 查看 系统 以了解您系统的信息。

33.4. 如何找到我的代理服务器设置?

要找到这些设置选项，请遵循下列步骤：

- Internet Explorer 8:
  1. 打开 Internet Explorer。
  2. 选择 工具 > Internet 选项.
  3. 在 连接 标签点击 局域网设置。
  4. 在 为 LAN 使用代理服务器 下面您会看到代理服务器的 地址 和 端口。
- Mozilla Firefox 3.6:
  1. 打开 Firefox。
  2. 选择 工具 > 选项。
  3. 在 高级 标签页，前往 网络 标签页。
  4. 点击 设置。
- 对 Opera 10.51:

1. 打开 Opera。
2. 选择 工具 > 偏好设置。
3. 在 高级 标签页，前往 网络 标签页。
4. 点击 代理服务器 按钮打开代理服务器设置对话框。

33.5. 如何彻底卸载 BitDefender?

请遵循以下步骤以正确卸载 BitDefender:

1. 前往 www.bitdefender.com/uninstall 下载卸载工具。
2. 用管理员权限运行卸载程序。
3. 重启您的电脑。

33.6. 如何启用/禁用实时防护?

BitDefender扫描所有被访问的文件、电子邮件消息和即时通讯流量，为您提供连续的实时防护，保证系统远离恶意软件。

通常 BitDefender 实时防护是开启的，您不应关闭它。

当您尝试诊断问题或删除病毒时，您可能需要禁用实时防护。比如如下情况:

- 安装 BitDefender 后电脑变慢问题
- 在安装 BitDefender 之后出现的某个程序问题。
- 在安装BitDefender 之后短期内会出现的错误消息

遵循以下步骤启用 / 临时禁用实时防护:

1. 打开 BitDefender，点击位于窗口右上角的 设置 并选择 专家视图。
2. 前往 反病毒 > 防护。
3. 清除 实时防护已启用 复选框以临时关闭反病毒实时防护（或选中它，如果您想启用防护）。
4. 您必须从菜单选择您希望实时防护被禁用的时间以确认您的选择。



注意
禁用 BitDefender 实时防护仅应被用作临时措施，且只禁用很短一段时间。

33.7. 如何显示 Windows 中的隐藏对象?

这些步骤对于您处理隐藏的感染文件有用。

参照以下步骤显示 Windows 中的隐藏对象:

1. 点击 开始，打开 控制面板 并选择 文件夹选项。

2. 前往 视图 标签。
3. 选择 显示系统文件夹内容 (仅适用于 Windows XP)。
4. 选择 显示隐藏文件及文件夹。
5. 清除 隐藏已知文件类型的扩展名。
6. 清除 隐藏受保护的操作系统文件。
7. 点击 应用 接着点击 确定。

词汇表

ActiveX

ActiveX 是一种写程序的模型，因此其他的程序和操作系统可以调用它。ActiveX技术被用于和 Microsoft Internet Explorer浏览器一起使用，来创建和计算机程序类似的交互型网页。使用ActiveX，用户可以提问或回答问题、使用按钮并可和网页用其他方式交互。ActiveX控件通常使用 Visual Basic 编写。

值得注意的是Active X 完全缺少安全控制；计算机安全专家不建议在网络中使用它。

广告软件

Adware（广告软件）一般是跟免费的宿主应用程序一起的，只要用户同意并接受Adware（广告软件）。因为Adware（广告软件）应用程序一般是在用户同意了一个说明了程序目的的授权使用协议之后才进行安装，因此并不算冒犯用户。

但是，弹出的广告可能非常恼人，有时甚至影响系统性能。此外，某些此类程序收集的信息可能侵犯用户隐私。

压缩包

含有已经被备份文件的磁盘，磁带或是目录。

它是一个含有一个或多个文件的压缩文件。

Backdoor （后门）

它是一个设计者或维修者故意留下的系统安全的漏洞。这样的漏洞的动机不一定总是恶意的，例如，有的操作系统在出厂时就留有给技术支持人员或维护人员留的特权账户。

Boot sector（引导扇区）

它是一个在每一个磁盘的头部的扇区，用以说明磁盘的体系结构（扇区大小，簇大小等等）。为了引导磁盘，引导扇区还包含载入操作系统的一段程序。

Boot virus（引导扇区病毒）

它是一个可以感染硬盘或软盘引导扇区的病毒。如果尝试从被引导扇区病毒感染的磁盘启动，那么将会导致此病毒在内存里活动。从这时起，当每次您启动您的系统时，病毒将会在内存里活动。

浏览

它是网络浏览器的简称。它是一个用作查找和显示网络网页的应用程序。两个最受欢迎的浏览器是：Netscape Navigator和微软Internet Explorer）。这两个浏览器都是图形界面，也就是说它们可以显示图像和文字。另外，现代多数的浏览器可以显示多媒体信息，包括声音和视频，虽然它们需要一些格式的插件。

Command line （命令行）

在命令行界面下，用户使用命令行语言在屏幕上直接输入命令。

Cookie

在互联网行业，Cookies是指您计算机上包含可被广告商用来追踪您的兴趣和爱好的信息的小文件。Cookie技术仍处于不断发展中，其目的是直接向您展示您感兴趣的广告。不过对很多人来说，这是一把双刃剑。一方面，您可有效地看到符合您兴趣的广告，另一方面，Cookie会跟踪并记录您访问了什么网页以及点击了什么地方。可以理解，会有有关隐私的争论，而且很多用户觉得Cookie被用作类似“条形码”的用途而感觉被冒犯。虽然此观点可能有点极端，但在某些情况下的确如此。

Disk drive （磁盘驱动器）

这是一个从磁盘上读写数据的设备。

硬盘驱动器可在硬盘上读写数据。

软盘驱动器可在软盘上读写数据。

磁盘驱动器可以是内置的（在计算机内部），也可以是外置的（连接到计算机上的外置设备）。

Download （下载）

从源主机往外围设备复制数据（通常是一个文件）的过程，此术语通常用来描述从在线服务向个人计算机复制文件的过程。此外，下载还可以指从网络文件服务器向网络中的计算机复制文件的过程。

E-mail(电子邮件)

Electronic mail的缩写。一种通过局域网或广域网在计算机上发送消息的服务。

事件

由程序检测到的操作或发生的事情。事件可能是用户操作，例如点击鼠标按钮或按下键盘等，也可能是系统中发生的事情，如内存溢出。

False positive （误报）

是指扫描程序将正常文件认定为受感染的文件。

Filename extension（文件扩展名）

它是文件名句号后的部分，表示文件类型。

许多操作系统（比如Unix，VMS，和MS-DOS）都用文件扩展名，它通常在一到三个字母之间。例如C源程序的“c”，PostScript语言的"ps",文本文件的"txt"。

Heuristic（启发式）

它是一个用来检测新病毒的基于规则的方法。该方式的扫描不需要依靠病毒库。启发式扫描的好处是不会被现存病毒的变种所欺骗。但是，它有可能报告一个正常程序中含有可疑代码，从而导致所谓的“误报” ("false positive")。

IP

网际网络协议（Internet Protocol） - 在TCP/IP 协议组里的一个路由协议，主要处理IP寻址、路由、分解及组装IP包。

Java applet（Java 小程序）

它是一个只在网页上运行的Java程序。为了要在网页上用Java 小程序，您需要指明这个Java 小程序的名字和Java 小程序可以利用的大小（长和宽，以像素为单位）。当一个含有Java 小程序的网页被访问时，浏览器会从服务器下载其Java 小程序并在客户端上运行。Java 小程序和应用程序不同，它被一个严格的安全协议所管理。

例如，尽管Java 小程序是在客户端上运行，但是它不可以读写客户端计算机。另外，小程序被进一步的约束着，所以它只可以在它所来自域名里进行数据读写。

Macro virus （宏病毒）

一种以宏命令方式嵌入文档中的电脑病毒，许多应用程序，如 Word 和 Excel，支持强大的宏语言。

这些程序允许在文档中嵌入宏，每次打开文档就将执行宏。

Mail client （电子邮件客户端程序）

电子邮件应用程序使用户可以编写、接收和发送邮件。

内存

计算机的内部存储区域，术语“内存”指以芯片方式存放的数据，“存储”是指存在于磁带或磁盘上的内存。每台计算机都带有一定数量的物理内存，通常被称为主存或 RAM。

Non-heuristic(非启发式)

这种扫描方式依赖病毒特征库，其优点是不会被看起来像是病毒的文件欺骗，因此很少产生误报。

Packed programs （加壳程序）

压缩后的文件。许多操作系统和应用程序都有可以压缩文件的指令以便减少内存使用。比如，一个文本文件包含10个连续的空格字符，通常就会需要10个字节存储。

但是，一个压缩程序会将空格字符替换为一个特殊的空格序列字符，然后跟上被替换的空格数。这样，10个空格字符只需两个字节存储。这只是一种加壳方式，还有很多其他的加壳方式。

路径

指打开系统内一个文件或文档的路径。通常，文档是从最高等级的开始分等级地分类。或指两个终点之间的路径，比如两台计算机之间的路径。

网络中任意两个网点之间有一个通道，如两台计算机之间的通讯渠道。

Phishing （钓鱼）

网上欺骗的一种方式。骗子伪装成合法公司的职员发送电子邮件给目标，意图要目标公开自己的个人资料，在此对资料进行偷窃。电子邮件会将目标连往一个网站，便要求目标输入合法公司已经拥有的各人资料（比如密码，信用卡，身份证号码和银行户口号码），这个网站是欺骗的工具。

Polymorphic virus （多形病毒）
可以侵略系统也同时可以变形的电脑病毒。这些病毒没有一定的二元图，也因此非常难查到。

端口
可以连接器材的端口。私人计算机共有几种端口。系统内部已有可连接硬盘，银幕和键盘的端口。系统外部又有可连接调制解调器，打印机，鼠标以及其他器材的端口。在TCP/IP和UDP网络内的终点，端口号数能指定用什么端口。

比如说，端口80是HTTP（WWW服务程序所用的协议）所用。在计算技术和通信技术中,网点上的一种功能部件,通过它数据可进入或离开一个数据网络或计算机。数据进出某功能部件的一种接口。

Report file （报告文件）
此文件列出已运用过的措施。BitDefender 保存着一个含有扫描过的路径，文件夹，存档和文件资料，以及受感染和可以文件的报告文件。

Rootkit（黑客工具）
Rootkit是一系列提供系统管理的软件工具.这个名词首先是在UNIX操作系统中出现的,指提供入侵管理权的编译工具,他们能隐藏自己不被系统管理员发现.

Rootkits 的主要作用是隐藏进程、文件、登录信息或日志，同时，如果正当的软件用于不正当的目的，它们也可从终端、网络连接或外设拦截数据。

Rootkits 本质上不具有恶意目的。例如，系统甚至某些应用程序会隐藏所使用的关键文件。然而，它经常用于隐藏恶意软件或系统闯入者的出现。当与恶意软件结合在一起时，Rootkits构成了对系统完整性和安全的最大威胁。它们可以监控流量、创建系统的后门，更改文件以及日志以避免被发现。

脚本
是宏或批量处理文件的另外一种名称。运用脚本不需用户者指令。

垃圾邮件
电子垃圾邮件或新闻组的垃圾新闻。一般它是指任何的未经过用户者同意就发送的邮件。

间谍软件
它是一种擅自通过网络联系累积用户者资料的软件。通常用于传送广告。它们通常潜入可从网上下载的免费或共享软件；不过大多数的免费或共享软件都不藏间谍软件。安装后，间谍软件会通过用户的网络联系把资料暗中传送出去。

这些软件有取得电子邮址，密码和信用卡号码的能力。间谍软件与木马相似的是用户都是在不知道的情况下安装它们的。

下载和安装对等的(peer-to-peer/p2p)软件是非常容易受间谍软件侵入的方式。除了采用不道德的方式偷取个人资料以外，间谍软件也会使用户的系统缓慢，使用系统的内存和网络联系宽带，长期内会使用户系统运行不顺畅，甚至是系统崩溃。

Startup items （启动项）

在这文件夹内的任何文件都会在系统启动时自行启动。启动时的屏幕，音响效果，日志或任何应用程序都能成为启动项。通常在此文件夹内的文件都是别名文件。

系统栏

系统托盘从 Windows 95 开始引入，位于 Windows 任务条右侧，包含访问系统功能及程序的小图标。双击或右键点击图标可以查看或访问程序细节功能。

TCP/IP （传输控制协议/互联网协议）

传输控制/互联网协议。用于不同操作系统，体系结构的网络基本协议。它定下了计算机之间的联络协议和条例，是互联网以及许多网络的通讯基础之一。

Trojan （木马）

伪装为良性程序的危险应用程序。此病毒种类并不会繁殖，但一样有危害性。最普遍的木马常伪装为反病毒软件，但其实是木马病毒。

一般此种病毒分成服务器端和客户端两部分，如计算机网络中服务器端被此程序感染，别人可通过网络其它计算机任意控制此计算机，并获得重要文件。国内流行的此类病毒有BO、NETSPY等。

更新

取代旧版本的新版本软件。另外，安装更新时，系统通常会确定旧版本已安装在系统内否则无法继续更新。

BitDefender拥有自己的更新模块让您指定或自动更新软件。

病毒

在您不知道的情况下存入系统并且启动的程序。多数的电脑病毒都能繁殖。所有的电脑病毒都是人造的。要创建一个会自己繁殖的电脑病毒并非一件难事。就连这样的简单病毒都有一定的危害性。它能够用尽系统的内存，使系统进入暂停的状态。更恶劣的病毒有通过网络联系以及保安措施的能力。计算机病毒实质上是指编制或在计算机程序中插入破坏计算机功能的数据，影响计算机使用并能自我复制的一组计算机指令或程序代码。一般病毒具有以下特性：可执行性——与其他合法程序一样，是一段可执行程序，但不是一个完整的程序，而是寄生在其他可执行程序上，当病毒运行时，便于合法程序争夺系统的控制权，往往会造成系统崩溃，导致计算机瘫痪。传染性——他通过各种渠道（磁盘、共享目录、邮件等）从已被感染的计算机扩散到其他机器上，在某种情况下导致计算机工作失常。潜伏性———一些编制精巧的病毒程序，进入系统之后不马上发作，隐藏在合法文件中，对其他系统进行秘密感染，一旦时机成熟，就四处繁殖、扩散。有的则执行格式化磁盘、删除磁盘文件、对数据文件进行加密等使系统死锁的操作。可触发性——病毒具有预定的触发条件，可能是时间、日期、文件类型或某些特定数据等。一旦满足触发感染的条件，它就会开始破坏工作，使病毒进行感染或攻击；如不满足，就会继续潜伏。针对性——有些病毒针对特定的操作系统或特定的计算机。隐蔽性——大部分病毒代码非常短小，也是为了隐蔽。一般都夹在正常程序之中，难以发现，一旦发作，则已经给计算机带来了不同程度的破坏 。

Virus definition （病毒库）
: 电脑病毒的二元图。反病毒软件用此找寻和消灭病毒。

Worm （蠕虫）
: 可以在网络上繁殖的程序。蠕虫不能潜入其他应用程序。